ADVANCED HIGHER ALGEBRA

CLASSICAL • MODERN
LINEAR • BOOLEAN

Important worked-out Examples added in this Edition

J. G. Chakravorty
P. R. Ghosh

NOBLE 102 YEARS
গৌরবময়
১০২
বছর

Publishing Books on MATHEMATICS since 1932

U.N. DHUR & SONS PRIVATE LTD.
KOLKATA 700 073

14th Edition

Thoroughly Revised and Enlarged according to the Latest CBCS Syllabus for B.Sc.(Honours) Courses for ALL SEMESTERS of All Indian Universities and other equivalent courses including Competitive Examinations.

ADVANCED HIGHER ALGEBRA

CLASSICAL • MODERN

LINEAR • BOOLEAN

J.G.Chakravorty, M.Sc., D.Phil.
P.R.Ghosh, M.Sc., D.Phil.

Serving the Academic Community since 1914

U.N.DHUR & SONS PRIVATE LTD.
KOLKATA - 700 073

CLASSICAL ALGEBRA

1 COMPLEX NUMBERS

1.1. Definitions.

The system of real numbers is not sufficient to solve all the algebraic equations. There are no real numbers which satisfy the equation $x^2+1=0$ or $x^2=-1$. In order to solve such equations, we extend the system of numbers and introduce a new class of numbers known as *imaginary* or *complex numbers*.

To cope with this idea, we introduce the symbol i to denote $\sqrt{-1}$ so that $i^2=-1$.

This i is not a real number. It is called the *fundamental imaginary unit*. We suppose that it combines with itself and with real numbers.

Any expression of the form $(a+ib)$, where a and b are both real, is called a *complex number*. Here the sign '+' does not indicate addition as usually understood. It is a mere symbol.

The real part of the complex number $(a+ib)$ is a and is written as $Re(a+ib)$, while its imaginary part is b and is written as $Imag\ (a+ib)$.

If $a=0$, then the complex number $(a+ib)$ becomes ib, which is purely imaginary. If $b=0$, then the complex number $(a+ib)$ becomes purely real. If both $a=0$ and $b=0$, then the complex number becomes zero. Hence the real numbers are particular cases of complex numbers.

If the real parts of two complex numbers be the same and their imaginary parts be same but of opposite signs, then the two numbers are said to be *complex conjugate numbers*. Thus $(a+ib)$ and $(a-ib)$ are complex conjugate numbers. If z be a complex number $(a+ib)$, then its conjugate $(a-ib)$ is denoted by $\bar{z}$. It is evident that conjugate of $\bar{z}$ is z.

3. (*i*) $7-4i$. (*ii*) $2(\sqrt{3}-1)-(\sqrt{3}+4)\,i$.

4. (*i*) 0. (*ii*) $2i$. (*iii*) $\frac{11}{4}$. (*iv*) i.

5. (*i*) $\pm\left(\sqrt{\frac{\sqrt{2}+1}{2}}+i\sqrt{\frac{\sqrt{2}-1}{2}}\right)$.

(*ii*) $\pm(2-2i)$. (*iii*) $\pm(5-6i)$. (*iv*) $\pm\frac{1}{\sqrt{2}}(1\pm i)$.

(*v*) $\pm\left(\sqrt{\frac{\sqrt{2+x^8-2x^4}+1}{2}}-i\sqrt{\frac{\sqrt{2+x^8-2x^4}-1}{2}}\right)$.

(*vi*) $\pm\{(a+b)-i(a-b)\}$. (*vii*) $\pm(x-\frac{1}{x}+2i)$.

(*viii*) $\pm(3+2i), \pm(2-3i)$.

6. (*c*) $\frac{1}{25}(18+i)$. (*e*) x^2+y^2. (*f*) 4.

7. $\frac{1}{2}(1+i\sqrt{11})$.

8. (*a*) $2(\cos\frac{1}{3}\pi+i\sin\frac{1}{3}\pi)$.

9. (*b*) $-\frac{9}{46}i, -\frac{3}{23}$.

16. (*b*) $\frac{1}{1-k^2}(k^2+i)\,;\left|\frac{k\sqrt{2}}{1-k^2}\right|$.

29. (*i*) $(a+ib)(a-ib)$. (*ii*) $(a-\omega b)(a-\omega^2 b)$.

(*iii*) $(a+b\omega+c\omega^2)(a+b\omega^2+c\omega)$.

(*iv*) $(a+b)(a+\omega b)(a+\omega^2 b)$.

1.9. De Moivre's theorem.

For all integral values of n, the value of $(\cos\theta+i\sin\theta)^n$ *is* $(\cos n\theta+i\sin n\theta)$ *and for all fractional values of n, one of the values of* $(\cos\theta+i\sin\theta)^n$ *is* $(\cos n\theta+i\sin n\theta)$.

Case. I. *When n is a positive integer.*

This is proved by the *method of induction.*

We have $(\cos\theta+i\sin\theta)^1=\cos\theta+i\sin\theta$

and $(\cos\theta+i\sin\theta)^2=\cos^2\theta-\sin^2\theta+2i\sin\theta\cos\theta$

$=\cos 2\theta+i\sin 2\theta$.

Therefore the theorem is true when $n=1$ and 2.

Let us assume that the theorem is true for a particular value m of n (m being a positive integer).

Then we have $(\cos\theta+i\sin\theta)^m=\cos m\theta+i\sin m\theta$.

Multiplying both sides by $(\cos\theta + i\sin\theta)$, we get

$$(\cos\theta + i\sin\theta)^{m+1} = (\cos m\theta + i\sin m\theta)(\cos\theta + i\sin\theta)$$
$$= (\cos m\theta\cos\theta - \sin m\theta\sin\theta) + i(\sin m\theta\cos\theta + \cos m\theta\sin\theta)$$
$$= \cos(m+1)\theta + i\sin(m+1)\theta.$$

Thus, if the theorem be true for $n = m$, it is also true for $n = m+1$. But it is proved that the theorem is true for $n = 2$. So it is also true for $n = 2+1 = 3$, then for $n = 3+1 = 4$ and so on. Hence the theorem is true for all positive integral values of n.

Case II. *When n is a negative integer.*

Let $n = -m$, where m is a positive integer.

Then $(\cos\theta + i\sin\theta)^n = (\cos\theta + i\sin\theta)^{-m}$

$$= \frac{1}{(\cos\theta + i\sin\theta)^m} = \frac{1}{\cos m\theta + i\sin m\theta}, \qquad \text{[by case I]}$$

$$= \frac{\cos m\theta - i\sin m\theta}{(\cos m\theta + i\sin m\theta)(\cos m\theta - i\sin m\theta)}$$

$$= \frac{\cos m\theta - i\sin m\theta}{\cos^2 m\theta + \sin^2 m\theta} = \cos m\theta - i\sin m\theta$$

$$= \cos(-n\theta) - i\sin(-n\theta) = \cos n\theta + i\sin n\theta.$$

Thus the theorem is true for all negative integral values of n.

Case III. *When n is a fraction, positive or negative.*

Let $n = \frac{p}{q}$, where q is a positive integer and p is any integer, positive or negative.

Then, by case I,

$$\left(\cos\frac{\theta}{q} + i\sin\frac{\theta}{q}\right)^q = \cos q\cdot\frac{\theta}{q} + i\sin q\cdot\frac{\theta}{q} = \cos\theta + i\sin\theta.$$

Extracting the q-th root of both sides, we see that one of the values of $(\cos\theta + i\sin\theta)^{\frac{1}{q}}$ is $\cos\frac{\theta}{q} + i\sin\frac{\theta}{q}$.

Raising both sides to p-th power, we can say that one of the values of $\{(\cos\theta+i\sin\theta)^{\frac{1}{q}}\}^p$, that is, of $(\cos\theta+i\sin\theta)^{\frac{p}{q}}$,

that is, of $(\cos\theta+i\sin\theta)^n$ is

$$(\cos\frac{\theta}{q}+i\sin\frac{\theta}{q})^p=\cos\frac{p}{q}\theta+i\sin\frac{p}{q}\theta=\cos n\theta+i\sin n\theta,$$

[by case I and case II].

Hence one of the values of $(\cos\theta+i\sin\theta)^n$ is $(\cos n\theta+i\sin n\theta)$.

Thus the theorem holds good for all rational values of n.

This theorem is known as *De Moivre's theorem*, named after its discoverer Prof. Abraham de Moivre.

Cor. 1. $(\cos\theta-i\sin\theta)^n=\{\cos(-\theta)+i\sin(-\theta)\}^n$

$$=\{(\cos\theta+i\sin\theta)^{-1}\}^n=(\cos\theta+i\sin\theta)^{-n}$$

$$=\cos(-n\theta)+i\sin(-n\theta)=\cos n\theta-i\sin n\theta.$$

Cor. 2. $(\cos m\theta+i\sin m\theta)^n=\{(\cos\theta+i\sin\theta)^m\}^n=(\cos\theta+i\sin\theta)^{mn}$

$$=\cos mn\theta+i\sin mn\theta=(\cos n\theta+i\sin n\theta)^m.$$

Note. The theorem actually holds for all real values of n. If n be irrational, then the total number of values of $(\cos\theta+i\sin\theta)^n$ will be infinite, but one of the values of $(\cos\theta+i\sin\theta)^n$ is $(\cos n\theta+i\sin n\theta)$.

1.10. Application of De Moivre's theorem.

(*a*) *Extraction of any assigned root of a complex number.*

Let $z=a+ib$ be the complex number. We put $a=r\cos\theta$ and $b=r\sin\theta$, so that $r=\sqrt{a^2+b^2}$ and $\theta=\tan^{-1}\frac{b}{a}$.

Then $z=a+ib=r(\cos\theta+i\sin\theta)=r\{\cos(\theta+2k\pi)+i\sin(\theta+2k\pi)\}$ for all integral values of k, since the expression $(\cos\theta+i\sin\theta)$ remains unaltered, if we put $(\theta+2k\pi)$ for θ.

Hence, by De Moivre's theorem, the n-th roots of z are

$$r^{\frac{1}{n}}\{\cos(2k\pi+\theta)+i\sin(2k\pi+\theta)\}^{\frac{1}{n}}=r^{\frac{1}{n}}\left(\cos\frac{2k\pi+\theta}{n}+i\sin\frac{2k\pi+\theta}{n}\right),$$

where $k=0,1,2,\ldots\ldots,(n-1)$.

If values greater than $(n-1)$, that is, $n, n+1, n+2, \ldots\ldots$ be given to k, then we would get the same quantities already obtained by putting $k=0,1,2,\ldots\ldots,(n-1)$ repeated over and over again.

Furthermore, no two quantities, as obtained by putting

$$k = 0, 1, 2, \ldots\ldots, (n-1),$$

are the same ; for, no two of the angles involved therein can have the same sine and same cosine. For, in these n quantities, no two of the angles are equal nor do they differ by a multiple of 2π.

Thus $\sqrt[n]{a+ib}$ has n distinct values

$$(a^2+b^2)^{\frac{1}{2n}}\left\{\cos\frac{1}{n}\left(2k\pi+\tan^{-1}\frac{b}{a}\right)+i\sin\frac{1}{n}\left(2k\pi+\tan^{-1}\frac{b}{a}\right)\right\},$$

where $k = 0, 1, 2, \ldots\ldots, (n-1)$.

Cor. To find the n-th roots of unity, we write

$1 = \cos 0 + i\sin 0 = \cos 2k\pi + i\sin 2k\pi$,where k is zero or any integer.

Hence $(1)^{\frac{1}{n}} = (\cos 2k\pi + i\sin 2k\pi)^{\frac{1}{n}} = \cos\dfrac{2k\pi}{n} + i\sin\dfrac{2k\pi}{n}$,

where $k = 0, 1, 2, \ldots\ldots, (n-1)$.

If n be even, then the real roots are ± 1 and the imaginary roots are

$$\cos\frac{2k\pi}{n} \pm i\sin\frac{2k\pi}{n}, \text{ where } k = 1, 2, \ldots\ldots, (\tfrac{1}{2}n-1).$$

If n be odd, then the real root is 1 only and the imaginary roots are

$$\cos\frac{2k\pi}{n} \pm i\sin\frac{2k\pi}{n}, \text{ where } k = 1, 2, \ldots\ldots, \tfrac{1}{2}(n-1).$$

(*b*) *Expansions of* $\cos n\theta$ *and* $\sin n\theta$ *, when n is a positive integer and* θ *is real.*

By De Moivre's theorem, we have

$$\cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n,$$

when n is a positive integer. Since $\cos\theta$ and $\sin\theta$ are both numerically less than 1 for all real values of θ, the expansion of $(\cos\theta + i\sin\theta)^n$ by Binomial theorem is valid and we therefore have

$$\begin{aligned}\cos n\theta + i\sin n\theta &= (\cos\theta + i\sin\theta)^n \\ &= \cos^n\theta + {}^nC_1\cos^{n-1}\theta(i\sin\theta) + {}^nC_2\cos^{n-2}\theta(i\sin\theta)^2 \\ &\qquad + {}^nC_3\cos^{n-3}\theta(i\sin\theta)^3 + \cdots\cdots + (i\sin\theta)^n \\ &= (\cos^n\theta - {}^nC_2\cos^{n-2}\theta\sin^2\theta + {}^nC_4\cos^{n-4}\theta\sin^4\theta - \cdots\cdots) \\ &\qquad + i({}^nC_1\cos^{n-1}\theta\sin\theta - {}^nC_3\cos^{n-3}\theta\sin^3\theta \\ &\qquad\qquad + {}^nC_5\cos^{n-5}\theta\sin^5\theta - \cdots\cdots).\end{aligned}$$

Equating the real and the imaginary parts from both sides, we get

$$\cos n\theta = \cos^n\theta - {}^nC_2 \cos^{n-2}\theta \sin^2\theta + {}^nC_4 \cos^{n-4}\theta \sin^4\theta - \cdots\cdots$$

and $\sin n\theta = {}^nC_1 \cos^{n-1}\theta \sin\theta - {}^nC_3 \cos^{n-3}\theta \sin^3\theta$

$$+ {}^nC_5 \cos^{n-5}\theta \sin^5\theta - \cdots\cdots .$$

If n be *odd*, then the last term in the expansion of $\cos n\theta$ is

$$(-1)^{\frac{n-1}{2}} {}^nC_{n-1} \cos\theta \sin^{n-1}\theta$$

and that of $\sin n\theta$ is $(-1)^{\frac{n-1}{2}} \sin^n\theta$.

If n be *even*, then the last term in the expansion of $\cos n\theta$ is

$$(-1)^{\frac{n}{2}} \sin^n\theta$$

and that of $\sin n\theta$ is $(-1)^{\frac{n-2}{2}} {}^nC_{n-1} \cos\theta \sin^{n-1}\theta$.

The series for $\cos n\theta$ and $\sin n\theta$ are thus *alternating*.

Cor. The expansion for $\tan n\theta$ can be obtained from the relation $\tan n\theta = \dfrac{\sin n\theta}{\cos n\theta}$ and by replacing $\sin n\theta$ and $\cos n\theta$ by their respective expansions. Thus we have $\tan n\theta = \dfrac{\sin n\theta}{\cos n\theta}$

$$= \frac{{}^nC_1 \cos^{n-1}\theta \sin\theta - {}^nC_3 \cos^{n-3}\theta \sin^3\theta + {}^nC_5 \cos^{n-5}\theta \sin^5\theta - \cdots}{\cos^n\theta - {}^nC_2 \cos^{n-2}\theta \sin^2\theta + {}^nC_4 \cos^{n-4}\theta \sin^4\theta - \cdots\cdots}$$

$$= \frac{n\tan\theta - {}^nC_3 \tan^3\theta + {}^nC_5 \tan^5\theta - \cdots\cdots}{1 - {}^nC_2 \tan^2\theta + {}^nC_4 \tan^4\theta - \cdots\cdots}$$

[Dividing both the numerator and the denominator by $\cos^n\theta$.]

(*c*) *Expansions of* $\cos\alpha$ *and* $\sin\alpha$ *in ascending powers of* α.

When n is a positive integer, we have

$$\cos n\theta = \cos^n\theta - {}^nC_2 \cos^{n-2}\theta \sin^2\theta + {}^nC_4 \cos^{n-4}\theta \sin^4\theta - \cdots\cdots$$

$$= \cos^n\theta - \frac{n(n-1)}{2!} \cos^{n-2}\theta \sin^2\theta$$

$$+ \frac{n(n-1)(n-2)(n-3)}{4!} \cos^{n-4}\theta \sin^4\theta - \cdots\cdots$$

and $\sin n\theta = n\cos^{n-1}\theta \sin\theta - \dfrac{n(n-1)(n-2)}{3!} \cos^{n-3}\theta \sin^3\theta$

$$+ \frac{n(n-1)(n-2)(n-3)(n-4)}{5!} \cos^{n-5}\theta \sin^5\theta - \cdots\cdots$$

Putting $n\theta = \alpha$, so that $n = \frac{\alpha}{\theta}$, we obtain

$$\cos\alpha = \cos^n\theta - \frac{\frac{\alpha}{\theta}\left(\frac{\alpha}{\theta}-1\right)}{2!}\cos^{n-2}\theta\sin^2\theta + \frac{\frac{\alpha}{\theta}\left(\frac{\alpha}{\theta}-1\right)\left(\frac{\alpha}{\theta}-2\right)\left(\frac{\alpha}{\theta}-3\right)}{4!}\cos^{n-4}\theta\sin^4\theta - \ldots\ldots$$

$$= \cos^n\theta - \frac{\alpha(\alpha-\theta)}{2!}\cos^{n-2}\theta\left(\frac{\sin\theta}{\theta}\right)^2 + \frac{\alpha(\alpha-\theta)(\alpha-2\theta)(\alpha-3\theta)}{4!}\cos^{n-4}\theta\left(\frac{\sin\theta}{\theta}\right)^4 - \ldots\ldots$$

and $$\sin\alpha = \alpha\cos^{n-1}\theta\left(\frac{\sin\theta}{\theta}\right) - \frac{\alpha(\alpha-\theta)(\alpha-2\theta)}{3!}\cos^{n-3}\theta\left(\frac{\sin\theta}{\theta}\right)^3 + \frac{\alpha(\alpha-\theta)(\alpha-2\theta)(\alpha-3\theta)(\alpha-4\theta)}{5!}\cos^{n-5}\theta\left(\frac{\sin\theta}{\theta}\right)^5 - \ldots\ldots$$

We measure θ and α in radians.

Keeping α fixed, if we make n to tend to infinity (positive), then θ tends to zero and $\frac{\sin\theta}{\theta}$ tends to 1.

Hence, in the limit, when $\theta \to 0$, we have

$$\cos\alpha = 1 - \frac{\alpha^2}{2!} + \frac{\alpha^4}{4!} - \ldots\ldots$$

and $$\sin\alpha = \alpha - \frac{\alpha^3}{3!} + \frac{\alpha^5}{5!} - \ldots\ldots$$

The expansions of $\cos\alpha$ and $\sin\alpha$ are thus both infinite series, which are easily found to be convergent.

We have

$$\cos\alpha^\circ = \cos\frac{\pi\alpha}{180} = 1 - \frac{1}{2!}\left(\frac{\pi\alpha}{180}\right)^2 + \frac{1}{4!}\left(\frac{\pi\alpha}{180}\right)^4 - \ldots\ldots$$

and $$\sin\alpha^\circ = \frac{\pi\alpha}{180} - \frac{1}{3!}\left(\frac{\pi\alpha}{180}\right)^3 + \frac{1}{5!}\left(\frac{\pi\alpha}{180}\right)^5 - \ldots\ldots$$

Cor. $\tan\alpha = \dfrac{\sin\alpha}{\cos\alpha} = (\sin\alpha)(\cos\alpha)^{-1}$

$$= \left(\alpha - \frac{\alpha^3}{3!} + \frac{\alpha^5}{5!} - \cdots\cdots\right)\left(1 - \frac{\alpha^2}{2!} + \frac{\alpha^4}{4!} - \cdots\cdots\right)^{-1}$$

$$= \left(\alpha - \frac{\alpha^3}{6} + \frac{\alpha^5}{120} - \cdots\cdots\right)\left\{1 + \left(\frac{\alpha^2}{2} - \frac{\alpha^4}{24} + \cdots\cdots\right) + \left(\frac{\alpha^2}{2} - \frac{\alpha^4}{24} + \cdots\cdots\right)^2 + \cdots\cdots\right\}.$$

Therefore $\tan\alpha = \alpha + \frac{1}{3}\alpha^3 + \frac{2}{15}\alpha^5 + \cdots\cdots$

(*d*) *Expression for* $\tan(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)$.

We have, by continued multiplication,

$$(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)(\cos\theta_3 + i\sin\theta_3)\ldots$$

$$\ldots(\cos\theta_n + i\sin\theta_n)$$

$$= \cos(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n) + i\sin(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)$$

or, $\cos(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n) + i\sin(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)$

$$= \cos\theta_1\cos\theta_2\cos\theta_3\cdots\cdots\cos\theta_n$$

$$\times(1 + i\tan\theta_1)(1 + i\tan\theta_2)(1 + i\tan\theta_3)\cdots\cdots(1 + i\tan\theta_n),$$

since $\cos\theta_r + i\sin\theta_r = \cos\theta_r(1 + i\tan\theta_r)$, $r = 1, 2, \ldots\ldots, n$

$$= \cos\theta_1\cos\theta_2\cos\theta_3\ldots\ldots\cos\theta_n\,(1 - ip_1 + i^2p_2 - \cdots\cdots + i^np_n),$$

where $p_r = \Sigma\tan\theta_1\tan\theta_2\tan\theta_3\ldots\ldots\tan\theta_r$, $r = 1, 2, 3, \ldots\ldots, n$

$$= \cos\theta_1\cos\theta_2\cos\theta_3\ldots\ldots\cos\theta_n$$

$$\times\{(1 - p_2 + p_4 - \cdots\cdots) + i(p_1 - p_3 + p_5 - \cdots\cdots)\}.$$

Equating the real and the imaginary parts from both sides, we get

$$\cos(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)$$

$$= \cos\theta_1\cos\theta_2\cos\theta_3\ldots\ldots\cos\theta_n\,(1 - p_2 + p_4 - \cdots\cdots)$$

and $\sin(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)$

$$= \cos\theta_1\cos\theta_2\cos\theta_3\ldots\ldots\cos\theta_n\,(p_1 - p_3 + p_5 - \cdots\cdots).$$

Therefore $\tan(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)$

$$= \frac{\sin(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)}{\cos(\theta_1 + \theta_2 + \theta_3 + \cdots\cdots + \theta_n)} = \frac{p_1 - p_3 + p_5 - \cdots\cdots}{1 - p_2 + p_4 - \cdots\cdots}.$$

(*e*) *Expansions of* $\cos^n\theta$ *and* $\sin^n\theta$ *when* n *is a positive integer and* θ *is real.*

Let $x = \cos\theta + i\sin\theta$.

Then, by De Moivre's theorem,

$$\frac{1}{x} = x^{-1} = (\cos\theta + i\sin\theta)^{-1} = \cos\theta - i\sin\theta,$$

$$x^n = (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$$

and $$\frac{1}{x^n} = x^{-n} = (\cos\theta + i\sin\theta)^{-n} = \cos n\theta - i\sin n\theta.$$

Therefore $x + \frac{1}{x} = 2\cos\theta$, $x - \frac{1}{x} = 2i\sin\theta$, $x^n + \frac{1}{x^n} = 2\cos n\theta$

and $$x^n - \frac{1}{x^n} = 2i\sin n\theta.$$

Hence $$(2\cos\theta)^n = \left(x + \frac{1}{x}\right)^n$$

$$= x^n + {}^nC_1\, x^{n-1}\frac{1}{x} + {}^nC_2\, x^{n-2}\frac{1}{x^2} + \cdots\cdots + {}^nC_{n-1}\, x\cdot\frac{1}{x^{n-1}} + \frac{1}{x^n}$$

$$= \left(x^n + \frac{1}{x^n}\right) + {}^nC_1\left(x^{n-2} + \frac{1}{x^{n-2}}\right) + {}^nC_2\left(x^{n-4} + \frac{1}{x^{n-4}}\right) + \cdots\cdots$$

or, $$2^n\cos^n\theta = 2\cos n\theta + {}^nC_1.2\cos(n-2)\theta + {}^nC_2.2\cos(n-4)\theta + \cdots\cdots$$

or, $$\cos^n\theta = 2^{1-n}\{\cos n\theta + {}^nC_1\cos(n-2)\theta + {}^nC_2\cos(n-4)\theta + \cdots\cdots\}.$$

Since n is a positive integer, the series on the right hand side is finite. Its last term will be a constant only or a constant multiple of $\cos\theta$ according as n is even or odd.

Also we have

$$(2i\sin\theta)^n = \left(x - \frac{1}{x}\right)^n$$

$$= x^n - {}^nC_1\, x^{n-2} + {}^nC_2\, x^{n-4} - \cdots\cdots$$

$$\cdots\cdots + (-1)^{n-1}\,{}^nC_{n-1}\cdot\frac{1}{x^{n-2}} + (-1)^n\cdot\frac{1}{x^n}.$$

If n be *even*, then we get

$$2^n(-1)^{\frac{n}{2}}\sin^n\theta = \left(x^n + \frac{1}{x^n}\right) - {}^nC_1\left(x^{n-2} + \frac{1}{x^{n-2}}\right)$$

$$+ {}^nC_2\left(x^{n-4} + \frac{1}{x^{n-4}}\right) - \cdots\cdots$$

$$= 2\cos n\theta - {}^nC_1\cdot 2\cos(n-2)\theta + {}^nC_2\cdot 2\cos(n-4)\theta - \cdots\cdots$$

or, $$\sin^n\theta = 2^{1-n}(-1)^{-\frac{n}{2}}\{\cos n\theta - {}^nC_1\cos(n-2)\theta + {}^nC_2\cos(n-4)\theta + \cdots\cdots\},$$

the last term of the series on the right hand side being a constant.

If n be *odd*, then we get

$$2^n \cdot i(-1)^{\frac{n-1}{2}} \sin^n\theta = \left(x^n - \frac{1}{x^n}\right) - {}^nC_1\left(x^{n-2} - \frac{1}{x^{n-2}}\right) + {}^nC_2\left(x^{n-4} - \frac{1}{x^{n-4}}\right) - \ldots\ldots$$

$$= 2i\sin n\theta - {}^nC_1 \cdot 2i\sin(n-2)\theta + {}^nC_2 \cdot 2i\sin(n-4)\theta - \ldots\ldots$$

or, $$\sin^n\theta = 2^{1-n}(-1)^{\frac{1-n}{2}}\{\sin n\theta - {}^nC_1\sin(n-2)\theta + {}^nC_2\sin(n-4)\theta - \ldots\ldots\},$$

the last term of the series on the right hand side containing $\sin\theta$ only.

1.11. Illustrative Examples.

Ex. 1. *Prove, by mathematical induction, that*

$$(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)\ldots\ldots(\cos\theta_n + i\sin\theta_n)$$
$$= \cos(\theta_1 + \theta_2 + \ldots\ldots + \theta_n) + i\sin(\theta_1 + \theta_2 + \ldots\ldots + \theta_n).$$

Hence deduce De Moivre's theorem for positive integral index.

By actual multiplication, we have

$$(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)$$
$$= (\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)$$
$$= \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2).$$

Therefore the theorem is true when $n = 2$.

Let us assume that the theorem is true for a particular value m of n (m being a positive integer). Then we have

$$(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)\ldots\ldots(\cos\theta_m + i\sin\theta_m)$$
$$= \cos(\theta_1 + \theta_2 + \ldots\ldots + \theta_m) + i\sin(\theta_1 + \theta_2 + \ldots\ldots + \theta_m).$$

Multiplying both sides by $(\cos\theta_{m+1} + i\sin\theta_{m+1})$, we get

$$(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)\cdots\cdots(\cos\theta_m + i\sin\theta_m)(\cos\theta_{m+1} + i\sin\theta_{m+1})$$
$$= \{\cos(\theta_1 + \theta_2 + \ldots\ldots + \theta_m) + i\sin(\theta_1 + \theta_2 + \ldots\ldots + \theta_m)\}(\cos\theta_{m+1} + i\sin\theta_{m+1})$$
$$= \cos(\theta_1 + \theta_2 + \ldots\ldots + \theta_m + \theta_{m+1}) + i\sin(\theta_1 + \theta_2 + \ldots\ldots + \theta_m + \theta_{m+1}),$$

by simple multiplication.

Thus, if the theorem be true for $n = m$, then it is also true for $n = m + 1$.

But it is proved that the theorem is true for $n = 2$. So it is also true for $n = 2 + 1 = 3$, then for $n = 3 + 1 = 4$ and so on. Hence the theorem is true for all positive integral values of n, that is, for any number of factors.

Putting $\theta_1 = \theta_2 = \cdots\cdots = \theta_n = \theta$ in this result, we get

$(\cos\theta + i\sin\theta)^n = \cos(\theta + \theta + \cdots\cdots \text{ to } n \text{ terms}) + i\sin(\theta + \theta + \cdots\cdots \text{ to } n \text{ terms})$

$= \cos n\theta + i\sin n\theta,$

which is De Moivre's theorem for positive integral index.

Ex. 2. *If n be a positive integer, then prove that*

$$\left(\frac{1+\sin\phi+i\cos\phi}{1+\sin\phi-i\cos\phi}\right)^n = \cos\left(\frac{n\pi}{2}-n\phi\right)+i\sin\left(\frac{n\pi}{2}-n\phi\right)$$

$$= (\sin\phi + i\cos\phi)^n. \qquad [\textit{C. H. 1963}]$$

We have $1+\sin\phi+i\cos\phi$

$= \sin^2\phi + \cos^2\phi + \sin\phi + i\cos\phi$

$= \sin^2\phi - i^2\cos^2\phi + \sin\phi + i\cos\phi$

$= (\sin\phi + i\cos\phi)(\sin\phi - i\cos\phi) + (\sin\phi + i\cos\phi)$

$= (\sin\phi + i\cos\phi)(\sin\phi - i\cos\phi + 1).$

Hence $\dfrac{1+\sin\phi+i\cos\phi}{1+\sin\phi-i\cos\phi} = \sin\phi + i\cos\phi$

or, $\left(\dfrac{1+\sin\phi+i\cos\phi}{1+\sin\phi-i\cos\phi}\right)^n = (\sin\phi + i\cos\phi)^n$

$$= \left\{\cos\left(\frac{\pi}{2}-\phi\right)+i\sin\left(\frac{\pi}{2}-\phi\right)\right\}^n$$

$$= \cos\left(\frac{n\pi}{2}-n\phi\right)+i\sin\left(\frac{n\pi}{2}-n\phi\right).$$

Ex. 3. *Simplify :* $\dfrac{(\cos\frac{1}{22}\pi + i\sin\frac{1}{22}\pi)^{11} \times (\cos\frac{1}{21}\pi - i\sin\frac{1}{21}\pi)^7}{(\cos\frac{1}{36}\pi + i\sin\frac{1}{36}\pi)^{12}}.$

By De Moivre's theorem, the given expression is equal to

$$\frac{(\cos\pi + i\sin\pi)^{\frac{11}{22}} \times (\cos\pi + i\sin\pi)^{-\frac{7}{21}}}{(\cos\pi + i\sin\pi)^{\frac{12}{36}}}$$

$= (\cos\pi + i\sin\pi)^{\frac{1}{2}-\frac{1}{3}-\frac{1}{3}} = (\cos\pi + i\sin\pi)^{-\frac{1}{6}}$

$= \cos\frac{1}{6}\pi - i\sin\frac{1}{6}\pi = \frac{1}{2}(\sqrt{3} - i).$

Ex. 4. (*a*) *Express* $\dfrac{(\cos\theta + i\sin\theta)^6}{(\sin\theta + i\cos\theta)^5}$ *in the form* $(A + iB)$.

(*b*) *Express* $\dfrac{-1+i\sqrt{3}}{1+i}$ *in polar form and then deduce the value of* $\cos\frac{5}{12}\pi$. [*C. H. 1986*].

(*a*) $\dfrac{(\cos\theta + i\sin\theta)^6}{(\sin\theta + i\cos\theta)^5} = (\cos\theta + i\sin\theta)^6 \{\cos(\frac{1}{2}\pi - \theta) + i\sin(\frac{1}{2}\pi - \theta)\}^{-5}$

$= (\cos 6\theta + i\sin 6\theta)\{\cos(-\frac{5}{2}\pi + 5\theta) + i\sin(-\frac{5}{2}\pi + 5\theta)\}$

$= \cos(-\frac{5}{2}\pi + 5\theta + 6\theta) + i\sin(-\frac{5}{2}\pi + 5\theta + 6\theta)$

$= \cos(4\pi - \frac{5}{2}\pi + 11\theta) + i\sin(4\pi - \frac{5}{2}\pi + 11\theta)$

$= \cos(\frac{3}{2}\pi + 11\theta) + i\sin(\frac{3}{2}\pi + 11\theta).$

(*b*) Let $-1 + i\sqrt{3} = r_1(\cos\theta_1 + i\sin\theta_1)$ and $1 + i = r_2(\cos\theta_2 + i\sin\theta_2)$, so that $r_1\cos\theta_1 = -1$, $r_1\sin\theta_1 = \sqrt{3}$ and $r_2\cos\theta_2 = 1$, $r_2\sin\theta_2 = 1$.

Therefore $r_1 = 2$, $\theta_1 = \frac{2}{3}\pi$ and $r_2 = \sqrt{2}$, $\theta_2 = \frac{1}{4}\pi$.

Hence $\dfrac{-1 + i\sqrt{3}}{1 + i} = \dfrac{r_1(\cos\theta_1 + i\sin\theta_1)}{r_2(\cos\theta_2 + i\sin\theta_2)} = \dfrac{2(\cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi)}{\sqrt{2}(\cos\frac{1}{4}\pi + i\sin\frac{1}{4}\pi)}$

$= \sqrt{2}(\cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi)(\cos\frac{1}{4}\pi + i\sin\frac{1}{4}\pi)^{-1}$

$= \sqrt{2}(\cos\frac{2}{3}\pi + i\sin\frac{2}{3}\pi)(\cos\frac{1}{4}\pi - i\sin\frac{1}{4}\pi)$

$= \sqrt{2}\{\cos(\frac{2}{3}\pi - \frac{1}{4}\pi) + i\sin(\frac{2}{3}\pi - \frac{1}{4}\pi)\}$

$= \sqrt{2}(\cos\frac{5}{12}\pi + i\sin\frac{5}{12}\pi).$

Therefore $\dfrac{-1 + i\sqrt{3}}{1 + i} = \dfrac{(-1 + i\sqrt{3})(1 - i)}{(1 + i)(1 - i)} = \dfrac{\sqrt{3} - 1}{2} + i\dfrac{\sqrt{3} + 1}{2}$

$= \sqrt{2}\cos\dfrac{5\pi}{12} + i\sqrt{2}\sin\dfrac{5\pi}{12}.$

Equating the real parts from both sides, we get

$$\sqrt{2}\cos\frac{5\pi}{12} = \frac{\sqrt{3} - 1}{2}, \text{ whence } \cos\frac{5\pi}{12} = \frac{\sqrt{3} - 1}{2\sqrt{2}}.$$

Ex. 5. *Find the cube roots of* (-1).

Let $x^3 = -1$

or, $x^3 = \cos\pi + i\sin\pi = \cos(2k\pi + \pi) + i\sin(2k\pi + \pi)$,

where $k = 0$, or any integer

or, $x = \{\cos(2k + 1)\pi + i\sin(2k + 1)\pi\}^{\frac{1}{3}}$

$= \cos\frac{1}{3}(2k + 1)\pi + i\sin\frac{1}{3}(2k + 1)\pi$, where $k = 0, 1, 2$.

Thus the required values are

$$\cos\tfrac{1}{3}\pi + i\sin\tfrac{1}{3}\pi,\ \cos\pi + i\sin\pi,\ \cos\tfrac{5}{3}\pi + i\sin\tfrac{5}{3}\pi$$

that is, $\frac{1}{2}(1 + i\sqrt{3})$, -1, $\frac{1}{2}(1 - i\sqrt{3})$.

Ex. 6. *Find the values of* $(1+i)^{\frac{1}{5}}$.

We have $1+i=\sqrt{2}\left(\frac{1}{\sqrt{2}}+i\frac{1}{\sqrt{2}}\right)=\sqrt{2}\left(\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}\right)$.

$$=2^{\frac{1}{2}}\{\cos(2k\pi+\tfrac{1}{4}\pi)+i\sin(2k\pi+\tfrac{1}{4}\pi)\},$$

where $k=0$, or any integer.

Hence $(1+i)^{\frac{1}{5}}=2^{\frac{1}{10}}\{\cos(2k\pi+\frac{1}{4}\pi)+i\sin(2k\pi+\frac{1}{4}\pi)\}^{\frac{1}{5}}$

$$=2^{\frac{1}{10}}\{\cos(2k+\tfrac{1}{4})\tfrac{1}{5}\pi+i\sin(2k+\tfrac{1}{4})\tfrac{1}{5}\pi\},\quad \text{where } k=0,1,2,3,4.$$

Ex. 7. *Solve* $x^7=1$.

We write $x^7=1=\cos 0+i\sin 0=\cos 2k\pi+i\sin 2k\pi$,

where $k=0$, or any integer

or, $x=(\cos 2k\pi+i\sin 2k\pi)^{\frac{1}{7}}=\cos\frac{2}{7}k\pi+i\sin\frac{2}{7}k\pi$,

where $k=0,1,2,3,4,5,6$.

Ex. 8. *Show that* $x^n-1=(x-1)\prod_{k=1}^{\frac{1}{2}(n-1)}\left(x^2-2x\cos\frac{2k\pi}{n}+1\right)$, *if* n *be an odd integer.*

We first find the roots of the equation $x^n-1=0$, that is, $x^n=1$.

Now, we write $x^n=1=\cos 2k\pi+i\sin 2k\pi$, where $k=0$, or any integer.

Therefore $x=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}$, where $k=0,1,2,\ldots\ldots,(n-1)$.

The only real root is corresponding to $k=0$ and that is 1.

The roots corresponding to $k=r$ and $k=n-r$, $(0<r<n)$, are $\cos\frac{2r\pi}{n}+i\sin\frac{2r\pi}{n}$ and $\cos\frac{2r\pi}{n}-i\sin\frac{2r\pi}{n}$ respectively.

They are conjugate and reciprocal to each other.

Hence the roots of the equation $x^n-1=0$ are

$$1,\ \cos\frac{2k\pi}{n}\pm i\sin\frac{2k\pi}{n},\ \text{where } k=1,2,\ldots\ldots,\frac{n-1}{2}.$$

Thus (x^n-1) can be expressed as the product of the factors

$$(x-1),\left\{x-\left(\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n}\right)\right\},\left\{x-\left(\cos\frac{2k\pi}{n}-i\sin\frac{2k\pi}{n}\right)\right\},$$

where $k=1,2,\ldots\ldots,\frac{n-1}{2}$.

Therefore $x^n - 1$

$$= (x-1)\prod_{k=1}^{\frac{1}{2}(n-1)}\left\{\left(x - \cos\frac{2k\pi}{n}\right) - i\sin\frac{2k\pi}{n}\right\}\left\{\left(x - \cos\frac{2k\pi}{n}\right) + i\sin\frac{2k\pi}{n}\right\}$$

$$= (x-1)\prod_{k=1}^{\frac{1}{2}(n-1)}\left(x^2 - 2x\cos\frac{2k\pi}{n} + 1\right).$$

Note. If n be an even integer, it can be shown similarly that

$$x^n - 1 = (x^2-1)\prod_{k=1}^{\frac{1}{2}(n-2)}\left(x^2 - 2x\cos\frac{2k\pi}{n} + 1\right).$$

Ex. 9. (a) *If* $z_r = \cos\frac{\pi}{2^r} + i\sin\frac{\pi}{2^r}$, *then prove that*

$$z_1 z_2 z_3 \ldots\ldots \text{ to } \infty = -1.$$

(b) *Find the general value of the real angle* θ *which satisfies the equation*

$$(\cos\theta + i\sin\theta)(\cos 2\theta + i\sin 2\theta)\ldots\ldots(\cos n\theta + i\sin n\theta) = 1.$$

[*B. H. 1988*]

(*a*) We have $z_1 z_2 z_3 \ldots\ldots \text{ to } \infty = \underset{n\to\infty}{Lt}\ (z_1 z_2 z_3 \ldots\ldots z_n)$

$$= \underset{n\to\infty}{Lt}\left(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\right)\left(\cos\frac{\pi}{2^2} + i\sin\frac{\pi}{2^2}\right)\ldots\ldots\left(\cos\frac{\pi}{2^n} + i\sin\frac{\pi}{2^n}\right)$$

$$= \cos\left(\frac{\pi}{2} + \frac{\pi}{2^2} + \frac{\pi}{2^3} + \ldots\ldots \text{ to } \infty\right) + i\sin\left(\frac{\pi}{2} + \frac{\pi}{2^2} + \frac{\pi}{2^3} + \ldots\ldots \text{ to } \infty\right)$$

$$= \cos\frac{\frac{1}{2}\pi}{1-\frac{1}{2}} + i\sin\frac{\frac{1}{2}\pi}{1-\frac{1}{2}} = \cos\pi + i\sin\pi = -1.$$

(*b*) We have

$$(\cos\theta + i\sin\theta)(\cos 2\theta + i\sin 2\theta)\cdots\cdots(\cos n\theta + i\sin n\theta) = 1$$

or, $\cos(\theta + 2\theta + \cdots\cdots + n\theta) + i\sin(\theta + 2\theta + \cdots\cdots + n\theta) = \cos 0 + i\sin 0$

or, $\cos\frac{1}{2}n(n+1)\theta + i\sin\frac{1}{2}n(n+1)\theta = \cos 2k\pi + i\sin 2k\pi,$

where $k = 0$, or any integer

or, $\frac{1}{2}n(n+1)\theta = 2k\pi$

or, $\theta = \frac{4k\pi}{n(n+1)}$, where $k = 0$, or any integer.

Ex. 10. *If* $x+\frac{1}{x}=2\cos\frac{\pi}{7}$, *then show that* $x^7+\frac{1}{x^7}=-2$.

We have $x+\frac{1}{x}=2\cos\frac{\pi}{7}$

or, $x^2+1=2x\cos\frac{1}{7}\pi$

or, $x^2-2x\cos\frac{1}{7}\pi+1=0$

or, $x=\frac{2\cos\frac{1}{7}\pi\pm\sqrt{4\cos^2\frac{1}{7}\pi-4}}{2}=\frac{2(\cos\frac{1}{7}\pi\pm i\sin\frac{1}{7}\pi)}{2}$

$=\cos\frac{1}{7}\pi\pm i\sin\frac{1}{7}\pi.$

Therefore $x^7=(\cos\frac{1}{7}\pi\pm i\sin\frac{1}{7}\pi)^7=\cos\pi\pm i\sin\pi=-1.$

Hence $x^7+\frac{1}{x^7}=-1+\frac{1}{-1}=-1-1=-2.$

Ex. 11. *If* $\cos\alpha+\cos\beta+\cos\gamma=0=\sin\alpha+\sin\beta+\sin\gamma$, *then prove that*

(*i*) $\cos 3\alpha+\cos 3\beta+\cos 3\gamma=3\cos(\alpha+\beta+\gamma)$

and $\sin 3\alpha+\sin 3\beta+\sin 3\gamma=3\sin(\alpha+\beta+\gamma).$ [*T. H. 2009*]

(*ii*) $\cos^2\alpha+\cos^2\beta+\cos^2\gamma=\sin^2\alpha+\sin^2\beta+\sin^2\gamma=\frac{3}{2}$.

[*C. H. 1988; B. H. 1994; T. H. 2009*]

Let $a=\cos\alpha+i\sin\alpha$, $b=\cos\beta+i\sin\beta$ and $c=\cos\gamma+i\sin\gamma$.

Therefore

$$a+b+c=(\cos\alpha+\cos\beta+\cos\gamma)+i(\sin\alpha+\sin\beta+\sin\gamma)=0.$$

(*i*) Now $a^3+b^3+c^3-3abc=(a+b+c)(a^2+b^2+c^2-ab-bc-ca)=0$

or, $a^3+b^3+c^3=3abc$

or, $(\cos\alpha+i\sin\alpha)^3+(\cos\beta+i\sin\beta)^3+(\cos\gamma+i\sin\gamma)^3$

$=3(\cos\alpha+i\sin\alpha)(\cos\beta+i\sin\beta)(\cos\gamma+i\sin\gamma)$

or, $\cos 3\alpha+i\sin 3\alpha+\cos 3\beta+i\sin 3\beta+\cos 3\gamma+i\sin 3\gamma$

$=3\{\cos(\alpha+\beta+\gamma)+i\sin(\alpha+\beta+\gamma)\}$

or, $(\cos 3\alpha+\cos 3\beta+\cos 3\gamma)+i(\sin 3\alpha+\sin 3\beta+\sin 3\gamma)$

$=3\{\cos(\alpha+\beta+\gamma)+i\sin(\alpha+\beta+\gamma)\}.$

Equating the real and the imaginary parts from both sides, we get

$$\cos 3\alpha+\cos 3\beta+\cos 3\gamma=3\cos(\alpha+\beta+\gamma)$$

and $$\sin 3\alpha+\sin 3\beta+\sin 3\gamma=3\sin(\alpha+\beta+\gamma).$$

(*ii*) We have $a^{-1}+b^{-1}+c^{-1}=\frac{1}{a}+\frac{1}{b}+\frac{1}{c}=\frac{bc+ca+ab}{abc}$.

Therefore $\frac{bc+ca+ab}{abc}=a^{-1}+b^{-1}+c^{-1}$

$=(\cos\alpha+i\sin\alpha)^{-1}+(\cos\beta+i\sin\beta)^{-1}+(\cos\gamma+i\sin\gamma)^{-1}$

$=\cos\alpha-i\sin\alpha+\cos\beta-i\sin\beta+\cos\gamma-i\sin\gamma$

$=(\cos\alpha+\cos\beta+\cos\gamma)-i(\sin\alpha+\sin\beta+\sin\gamma)=0$

or, $bc+ca+ab=0$.

Now $a^2+b^2+c^2=(a+b+c)^2-2(bc+ca+ab)=0$

or, $(\cos\alpha+i\sin\alpha)^2+(\cos\beta+i\sin\beta)^2+(\cos\gamma+i\sin\gamma)^2=0$

or, $(\cos 2\alpha+\cos 2\beta+\cos 2\gamma)+i(\sin 2\alpha+\sin 2\beta+\sin 2\gamma)=0$.

Hence the real and the imaginary parts are each equal to zero.

Thus $\cos 2\alpha+\cos 2\beta+\cos 2\gamma=0$

or, $\cos^2\alpha-\sin^2\alpha+\cos^2\beta-\sin^2\beta+\cos^2\gamma-\sin^2\gamma=0$

or, $\cos^2\alpha+\cos^2\beta+\cos^2\gamma=\sin^2\alpha+\sin^2\beta+\sin^2\gamma=k$ (say).

Therefore

$2k=\cos^2\alpha+\cos^2\beta+\cos^2\gamma+\sin^2\alpha+\sin^2\beta+\sin^2\gamma=1+1+1=3$.

Therefore $k=\frac{3}{2}$.

Hence $\cos^2\alpha+\cos^2\beta+\cos^2\gamma=\sin^2\alpha+\sin^2\beta+\sin^2\gamma=\frac{3}{2}$.

Ex. 12. *If* $(1+x)^n=a_0+a_1x+a_2x^2+a_3x^3+\ldots\ldots$, *then show that*

$a_0-a_2+a_4-\ldots\ldots=2^{\frac{n}{2}}\cos\frac{1}{4}n\pi$ *and* $a_1-a_3+a_5-\ldots\ldots=2^{\frac{n}{2}}\sin\frac{1}{4}n\pi$.

We have $(1+x)^n=a_0+a_1x+a_2x^2+a_3x^3+\ldots\ldots$

Putting $x=i$, we get $(1+i)^n=a_0+a_1i+a_2i^2+a_3i^3+\ldots\ldots$

or, $\{\sqrt{2}(\cos\frac{1}{4}\pi+i\sin\frac{1}{4}\pi)\}^n=a_0+a_1i-a_2-a_3i+\ldots\ldots$

or, $2^{\frac{n}{2}}(\cos\frac{1}{4}n\pi+i\sin\frac{1}{4}n\pi)=(a_0-a_2+a_4-\ldots\ldots)+i(a_1-a_3+a_5-\ldots\ldots)$.

Equating the real and the imaginary parts from both sides, we get

$a_0-a_2+a_4-\ldots\ldots=2^{\frac{n}{2}}\cos\frac{1}{4}n\pi$ and $a_1-a_3+a_5-\ldots\ldots=2^{\frac{n}{2}}\sin\frac{1}{4}n\pi$.

Ex. 13. (*a*) *If* $a=\cos\alpha+i\sin\alpha$ *and* n *be a positive integer, then prove that* $a^n+\frac{1}{a^n}=2\cos n\alpha$ *and* $a^n-\frac{1}{a^n}=2i\sin n\alpha$.

Hence show that $64\sin^4\alpha\cos^3\alpha=\cos 7\alpha-\cos 5\alpha-3\cos 3\alpha+3\cos\alpha$.

(b) *Expand* $\cos^7\theta$ *in a series of cosines of multiples of* θ. [*B. H. 1995*]

(*a*) We have $a = \cos\alpha + i\sin\alpha$.

Therefore $a^n = (\cos\alpha + i\sin\alpha)^n = \cos n\alpha + i\sin n\alpha$

and $\frac{1}{a^n} = a^{-n} = (\cos\alpha + i\sin\alpha)^{-n} = \cos n\alpha - i\sin n\alpha.$

Hence $a^n + \frac{1}{a^n} = 2\cos n\alpha$ and $a^n - \frac{1}{a^n} = 2i\sin n\alpha.$

So we have $2\cos\alpha = a + \frac{1}{a}$ and $2i\sin\alpha = a - \frac{1}{a}$.

Therefore $(2i\sin\alpha)^4(2\cos\alpha)^3 = \left(a - \frac{1}{a}\right)^4\left(a + \frac{1}{a}\right)^3$

or, $2^4 i^4 \sin^4\alpha . 2^3\cos^3\alpha = \left(a - \frac{1}{a}\right)\left(a^2 - \frac{1}{a^2}\right)^3 = \left(a - \frac{1}{a}\right)\left(a^6 - 3a^2 + \frac{3}{a^2} - \frac{1}{a^6}\right)$

or, $2^7\sin^4\alpha\cos^3\alpha = \left(a^7 + \frac{1}{a^7}\right) - \left(a^5 + \frac{1}{a^5}\right) - 3\left(a^3 + \frac{1}{a^3}\right) + 3\left(a + \frac{1}{a}\right)$

or, $128\sin^4\alpha\cos^3\alpha = 2\cos 7\alpha - 2\cos 5\alpha - 3.2\cos 3\alpha + 3.2\cos\alpha$

or, $64\sin^4\alpha\cos^3\alpha = \cos 7\alpha - \cos 5\alpha - 3\cos 3\alpha + 3\cos\alpha$.

(*b*) Let $x = \cos\theta + i\sin\theta$; so that

$\frac{1}{x} = \cos\theta - i\sin\theta$, $x^n = \cos n\theta + i\sin n\theta$ and $\frac{1}{x^n} = \cos n\theta - i\sin n\theta$.

Therefore $x^n + \frac{1}{x^n} = 2\cos n\theta$ and $x + \frac{1}{x} = 2\cos\theta$.

Now $(2\cos\theta)^7 = \left(x + \frac{1}{x}\right)^7$

$$= x^7 + 7x^5 + 21x^3 + 35x + \frac{35}{x} + \frac{21}{x^3} + \frac{7}{x^5} + \frac{1}{x^7}$$

$$= \left(x^7 + \frac{1}{x^7}\right) + 7\left(x^5 + \frac{1}{x^5}\right) + 21\left(x^3 + \frac{1}{x^3}\right) + 35\left(x + \frac{1}{x}\right)$$

$$= 2\cos 7\theta + 7 . 2\cos 5\theta + 21 . 2\cos 3\theta + 35 . 2\cos\theta$$

or, $\cos^7\theta = \frac{1}{64}(\cos 7\theta + 7\cos 5\theta + 21\cos 3\theta + 35\cos\theta)$.

Ex. 14. *Find the limit of* $\dfrac{3\sin\theta-\sin 3\theta}{\theta-\sin\theta}$ *as* θ *tends to zero.*

From the expansion of $\sin\theta$, we have

$$\frac{3\sin\theta-\sin 3\theta}{\theta-\sin\theta}=\frac{3\left(\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\cdots\cdots\right)-\left(3\theta-\frac{3^3\theta^3}{3!}+\frac{3^5\theta^5}{5!}-\cdots\cdots\right)}{\theta-\left(\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\cdots\cdots\right)}$$

$$=\frac{\frac{\theta^3}{3!}(3^3-3)-\frac{\theta^5}{5!}(3^5-3)+\cdots\cdots}{\frac{\theta^3}{3!}-\frac{\theta^5}{5!}+\cdots\cdots}=\frac{\frac{1}{3!}(3^3-3)-\frac{\theta^2}{5!}(3^5-3)+\cdots\cdots}{\frac{1}{3!}-\frac{\theta^2}{5!}+\cdots\cdots}.$$

Therefore $\underset{\theta\to 0}{Lt}\dfrac{3\sin\theta-\sin 3\theta}{\theta-\sin\theta}=\dfrac{\frac{1}{3!}(3^3-3)}{\frac{1}{3!}}=24.$

Ex. 15. *Find* θ, *when* $\dfrac{\sin\theta}{\theta}=\dfrac{3239}{3240}$. [*N. B. H. 2004*]

Since $\dfrac{\sin\theta}{\theta}=\dfrac{3239}{3240}\simeq 1$, θ is very small and so higher powers of θ above the second may be neglected. Hence, from the expansion of $\sin\theta$, we have

$$\frac{3239}{3240}=\frac{\sin\theta}{\theta}=\frac{\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\cdots\cdots}{\theta}=1-\frac{\theta^2}{3!}$$

or, $\dfrac{1}{6}\theta^2=1-\dfrac{3239}{3240}=\dfrac{1}{3240}$

or, $\theta^2=\dfrac{1}{540}$, whence $\theta=\dfrac{1}{23\cdot 24}$ radian (nearly) $=2^0\cdot 46$ (nearly).

Examples I (B)

1. Simplify :

(*i*) $\dfrac{(\cos 2\theta+i\sin 2\theta)^9(\cos 3\theta-i\sin 3\theta)^5}{(\cos 4\theta+i\sin 4\theta)^3(\cos\theta-i\sin\theta)^9}$.

(*ii*) $\left(\dfrac{\cos\theta-i\sin\theta}{\sin\theta-i\cos\theta}\right)^3$.

(*iii*) $\dfrac{(\cos\theta+i\sin\theta)^9}{(\cos\theta-i\sin\theta)^4}$.

(*iv*) $\{\cos\alpha-\cos\beta+i(\sin\alpha-\sin\beta)\}^n$
$+\{\cos\alpha-\cos\beta-i(\sin\alpha-\sin\beta)\}^n$.

(*v*) $\dfrac{(\cos\frac{1}{15}\pi+i\sin\frac{1}{15}\pi)^{10}+(\cos\frac{1}{15}\pi-i\sin\frac{1}{15}\pi)^{10}}{(\cos\frac{1}{3}\pi+i\sin\frac{1}{3}\pi)^6}$.

(*vi*) $(1+\cos\theta+i\sin\theta)^n$.

(*vii*) $\left(\dfrac{1+\cos\theta+i\sin\theta}{1+\cos\theta-i\sin\theta}\right)^n$. (*viii*) $\left(\dfrac{i+i\sin\theta+\cos\theta}{1+\sin\theta+i\cos\theta}\right)^5$.

2. Find the values of the following :

(*i*) $(1)^{\frac{1}{3}}$. (*ii*) $(64)^{\frac{1}{6}}$. (*iii*) $(i)^{\frac{3}{4}}$. (*iv*) $(-i)^{\frac{3}{5}}$.

(*v*) $(1-i)^7$. (*vi*) $\dfrac{3}{(2+i)^3}$. (*vii*) $(\sqrt{3}-i)^{\frac{1}{7}}$.

(*viii*) $(1+i\sqrt{3})^{\frac{1}{2}}$. (*ix*) $(-8)^{\frac{1}{6}}$.

3. (*a*) Express $P=\dfrac{(\sqrt{3}-1)+i(\sqrt{3}+1)}{2\sqrt{2}}$ in the form $r(\cos\theta+i\sin\theta)$ and derive all the four values of $P^{\frac{1}{4}}$.

(*b*) Express $P=32\sqrt{2}\,\{\sqrt{3}(1+i)+(1-i)\}$ in the polar form.

Finally calculate all the seven values of $P^{\frac{1}{7}}$.

4. (*a*) Show that one of the values of

$$(1+i\sqrt{3})^{\frac{3}{4}}+(1-i\sqrt{3})^{\frac{3}{4}} \text{ is } \sqrt[4]{32}\,.$$

(*b*) Show that the product of all the values of $(1+i\sqrt{3})^{\frac{3}{4}}$ is 8.

[*C. H. 1981, 2004 ; B. H. 1994*]

5. If n be a positive integer, then prove that

(*i*) $(1+i)^n+(1-i)^n=2^{\frac{n}{2}+1}\cos\frac{1}{4}n\pi$.

(*ii*) $(a+ib)^n+(a-ib)^n=2(a^2+b^2)^{\frac{n}{2}}\cos\left(n\tan^{-1}\dfrac{b}{a}\right)$.

6. Solve :

(*i*) $x^5=1$. (*ii*) $x^{12}+a^{12}=0$.

(*iii*) $x^5+x^4+x^3+x^2+x+1=0$. [*T. H. 2009*]

(*iv*) $x^4+(1-x)^4=0$. (*v*) $x^3=8(1-x)^3$.

(*vi*) $(1+x)^6+x^6=0$. (*vii*) $x^8+x^5-x^3-1=0$.

(*viii*) $(1+x)^n=(1-x)^n$. [*C. H. 1965*]

7. Find the roots of the equation $z^n = (z+1)^n$ and show that the points which represent them in the Argand diagram are collinear.

[C. H. 1985 ; N. B. H. 1986, 1988 ; V. H. 1989 ; K. H. 2002]

8. Show that the seven numbers

$$\cos \tfrac{1}{7}(2n+1)\pi + i \sin \tfrac{1}{7}(2n+1)\pi, \ (n = 0, 1, 2, \ldots\ldots, 6)$$

are distinct and each is a seventh root of (-1).

9. Find the real factors of the following :

(*i*) $x^5 + 1$. (*ii*) $x^{2n} + 1$.

(*iii*) $x^n + 1$, where n is an odd integer. [C. H. 1965]

10. Find the general values of the real angle θ which will satisfy the equation

(*i*) $(\cos\theta + i\sin\theta)(\cos 3\theta + i \sin 3\theta) \ldots\ldots$

$$\ldots\ldots \{\cos(2n-1)\theta + i\sin(2n-1)\theta\} = 1.$$

(*ii*) $(\cos\theta + i\sin\theta)(\cos 2\theta + i\sin 2\theta) \ldots\ldots (\cos n\theta + i \sin n\theta) = -i$.

11. (*a*) If $x = \cos\theta + i\sin\theta$, $y = \cos\phi + i\sin\phi$, then prove that $\dfrac{x^m}{y^n} + \dfrac{y^n}{x^m} = 2\cos(m\theta - n\phi)$, where m and n are integers. [K. H..2000]

(*b*) If $x_r = \cos\theta_r + i\sin\theta_r$, $(r = 1, 2, \ldots\ldots, n)$, then show that

(*i*) $x_1 x_2 \ldots\ldots x_n + \dfrac{1}{x_1 x_2 \ldots\ldots x_n} = 2\cos(\theta_1 + \theta_2 + \ldots\ldots + \theta_n)$.

(*ii*) $x_1^{p_1} x_2^{p_2} \ldots\ldots x_n^{p_n} + \dfrac{1}{x_1^{p_1} x_2^{p_2} \ldots\ldots x_n^{p_n}}$

$$= 2\cos(p_1\theta_1 + p_2\theta_2 + \ldots\ldots + p_n\theta_n),$$

where p_r, $(r = 1, 2, \ldots\ldots, n)$, are rational numbers.

(*iii*) $\dfrac{1}{x_1} + \dfrac{1}{x_2} + \ldots\ldots + \dfrac{1}{x_n} = 0$, if $x_1 + x_2 + \ldots\ldots + x_n = 0$.

(*c*) If $x_r = \cos 2\theta_r + i\sin 2\theta_r$, $(r = 1, 2, 3, 4)$, then show that

$$\sqrt{\frac{x_1 x_2}{x_3 x_4}} + \sqrt{\frac{x_3 x_4}{x_1 x_2}} = 2\cos(\theta_1 + \theta_2 - \theta_3 - \theta_4).$$

12. If $x_r = \cos r\theta + i\sin r\theta$, $(r = 1, 2, \ldots\ldots, n)$, then show that $x_1, x_2, x_3, \ldots\ldots, x_n$ are in G. P.

13. (*a*) If $\alpha = \cos\frac{2r\pi}{n} + i\sin\frac{2r\pi}{n}$ and if r and p be prime to n, then prove that $1 + \alpha^p + \alpha^{2p} + \ldots\ldots + \alpha^{(n-1)p} = 0$. [*C. H. 1967; B. H. 1994*]

(*b*) If $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_7$ be the roots of the equation $x^7 + 1 = 0$, then show that $\alpha_1^{100} + \alpha_2^{100} + \alpha_3^{100} + \ldots\ldots + \alpha_7^{100} = 0$. [*B. H. 1996*]

14. If $z_r = \cos\frac{\pi}{3^r} + i\sin\frac{\pi}{3^r}$, $(r = 1, 2, \ldots\ldots)$, then prove that

$$z_1 z_2 z_3 \ldots\ldots \text{ to infinity} = i.$$

15. If $\cos\theta = \frac{1}{2}\left(a + \frac{1}{a}\right)$ and $\cos\phi = \frac{1}{2}\left(b + \frac{1}{b}\right)$, then show that $\cos(\theta + \phi)$ is one of the values of $\frac{1}{2}\left(ab + \frac{1}{ab}\right)$.

16. (*a*) If $x_r = \cos\alpha_r + i\sin\alpha_r$, $(r = 1, 2, 3)$, then show that

$$\frac{(x_1 + x_2)(x_2 + x_3)(x_3 + x_1)}{x_1 x_2 x_3} \text{ is real and is equal to}$$

$$8\cos\tfrac{1}{2}(\alpha_1 - \alpha_2)\cos\tfrac{1}{2}(\alpha_2 - \alpha_3)\cos\tfrac{1}{2}(\alpha_3 - \alpha_1).$$

(*b*) If $x + \frac{1}{x} = 2\cos\alpha$, $y + \frac{1}{y} = 2\cos\beta$, $z + \frac{1}{z} = 2\cos\gamma$, then prove that

(*i*) $\Sigma\sin\alpha\cos\alpha = 0$, $\Sigma\sin(\beta + \gamma) = 0$, $\Sigma\cos(\beta + \gamma) = 0$, $\Sigma\sin 4\alpha = 2\,\Sigma\sin 2(\beta + \gamma)$ and $\Sigma\cos 4\alpha = 2\,\Sigma\cos 2(\beta + \gamma)$, if $x + y + z = 0$.

(*ii*) $\Sigma\cos(\beta - \gamma) = -1$, if $x + y + z = xyz$. [*B. H. 1993*]

17. (*a*) If $(1 + x)^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots\ldots$, then show that

$$a_0 + a_4 + a_8 + \ldots\ldots = 2^{n-2} + 2^{\frac{n}{2}-1}\cos\tfrac{1}{4}n\pi.$$

(*b*) Show that $1 - {}^nC_2 + {}^nC_4 - \ldots\ldots = 2^{\frac{n}{2}}\cos\tfrac{1}{4}n\pi$

and $\quad {}^nC_1 - {}^nC_3 + {}^nC_5 - \ldots\ldots = 2^{\frac{n}{2}}\sin\tfrac{1}{4}n\pi.$

(*c*) If $(1 + x)^n = a_0 + a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n$ and

$S_1 = a_0 + a_3 + a_6 + \ldots\ldots$, $S_2 = a_1 + a_4 + a_7 + \ldots\ldots$, $S_3 = a_2 + a_5 + a_8 + \ldots\ldots$,

then show that the values of S_1, S_2, S_3 are $\frac{1}{3}\left(2^n + 2\cos\frac{r\pi}{3}\right)$,

where $r = n, n - 2, n + 2$ respectively. [*V. H. 1991*]

18. If $(a_1 + i\,b_1)\,(a_2 + i\,b_2)\,\ldots\ldots\,(a_n + i\,b_n) = A + i\,B$, then show that

(*i*) $(a_1^{\,2} + b_1^{\,2})\,(a_2^{\,2} + b_2^{\,2})\,\ldots\ldots\,(a_n^{\,2} + b_n^{\,2}) = A^{\,2} + B^{\,2}$.

(*ii*) $\tan^{-1}\dfrac{b_1}{a_1} + \tan^{-1}\dfrac{b_2}{a_2} + \ldots\ldots + \tan^{-1}\dfrac{b_n}{a_n} = \tan^{-1}\dfrac{B}{A}$. [*T. H. 2009*]

19. What is the principal value of the amplitude of

$$(\cos 50^\circ + i \sin 50^\circ)^6 ?$$

20. If $x = \cos\theta + i \sin\theta$ and $1 + \sqrt{1 - a^{\,2}} = na$, then prove that

$$1 + a\cos\theta = \frac{a}{2n}(1 + nx)\left(1 + \frac{n}{x}\right).$$

21. From the identity

$$a^{\,2}\frac{(x-b)(x-c)}{(a-b)(a-c)} + b^{\,2}\frac{(x-c)(x-a)}{(b-c)(b-a)} + c^{\,2}\frac{(x-a)(x-b)}{(c-a)(c-b)} = x^{\,2},$$

deduce the following identities :

(*i*) $\cos 2(\theta+\alpha)\dfrac{\sin(\theta-\beta)\sin(\theta-\gamma)}{\sin(\alpha-\beta)\sin(\alpha-\gamma)} + \ldots\ldots = \cos 4\theta$

and (*ii*) $\sin 2(\theta+\alpha)\dfrac{\sin(\theta-\beta)\sin(\theta-\gamma)}{\sin(\alpha-\beta)\sin(\alpha-\gamma)} + \ldots\ldots = \sin 4\theta.$

22. If n be a positive integer and $(7 + 2i)^n = a + ib$, then prove that $a^{\,2} + b^{\,2} = 53^{\,n}$. Hence express $53^{\,3}$ as the sum of two squares.

23. (*a*) Show that the sum of the 99-th powers of the roots of the equation $x^{\,5} = 1$ is zero. [*C. H. 1969*]

(*b*) Prove that the sum of the n-th powers of the roots of the equation $x^{\,7} = 1$, n being an integer not divisible by 7, is zero .

24. (*a*) If α and β be the roots of the equation

$$x^{\,2} - 2x\cos\theta + 1 = 0,$$

then find the equation whose roots are $\alpha^{\,n}$ and $\beta^{\,n}$.

(*b*) Find the equation whose roots are the n-th powers of those of the equation $x^{\,2} - 2x + 4 = 0$. [*B. H. 1995*]

Show that the sum of the n-th powers of the roots is

$$2^{n+1}\cos\frac{n\pi}{3}.$$ [*C. H. 1980*]

25. (*a*) Solving the equation $x^7 - 1 = 0$, deduce that $2\cos\frac{2}{7}\pi$, $2\cos\frac{4}{7}\pi$ and $2\cos\frac{8}{7}\pi$ are the roots of the equation $t^3 + t^2 - 2t - 1 = 0$.

(*b*) If $2\cos\frac{1}{7}\pi$ be a root of the equation $x^3 - x^2 - 2x + 1 = 0$, then find its other roots.

(*c*) Prove that the roots of the equation

$$x^{10} + 11x^5 - 1 = 0$$

are the values of $\frac{\pm\sqrt{5}-1}{2}\left(\cos\frac{2k\pi}{5} + i\sin\frac{2k\pi}{5}\right)$, where $k = 0, 1, 2, 3, 4$.

[From the given equation, $x^5 = \frac{1}{2}(-11 \pm \sqrt{125}) = \{\frac{1}{2}(\pm\sqrt{5} - 1)\}^5$.]

26. (*a*) Prove that the roots of the equation $x^3 - 3x + 1 = 0$ are

$$2\cos\tfrac{2}{9}\pi,\ 2\cos\tfrac{8}{9}\pi \text{ and } 2\cos\tfrac{14}{9}\pi.$$

(*b*) Find the equation whose roots are

$$\cos\tfrac{2}{7}\pi,\ \cos\tfrac{4}{7}\pi,\ \cos\tfrac{6}{7}\pi.$$

27. Show that the roots of the equation $x^7 = 1$ are the multiples of a, where $a = \cos\frac{2}{7}\pi + i\sin\frac{2}{7}\pi$. Also prove that the roots of the equation $x^2 + x + 2 = 0$ are $(a + a^2 + a^4)$ and $(a^3 + a^5 + a^6)$.

28. With the help of De Moivre's theorem,

(*a*) find the formulae for $\cos 3\theta$ and $\sin 3\theta$;

(*b*) expand (*i*) $\sin 7\theta$ in powers of $\sin\theta$,

(*ii*) $\cos 5\theta$ in powers of $\cos\theta$

and (*iii*) $\tan 5\theta$ in terms of $\tan\theta$.

29. (*a*) Expand $\cos^5\theta$ and $\cos^6\theta$ in cosines of multiples of θ.

(*b*) Expand $\sin^5\theta$ and $\sin^7\theta$ in sines of multiples of θ.

30. Prove that

(*i*) $64\sin^5\theta\cos^2\theta = \sin 7\theta - 3\sin 5\theta + \sin 3\theta + 5\sin\theta$.

(*ii*) $32\sin^4\theta\cos^2\theta = \cos 6\theta - 2\cos 4\theta - \cos 2\theta + 2$.

(*iii*) $1 + \cos 10\theta = 2(16\cos^5\theta - 20\cos^3\theta + 5\cos\theta)^2$.

31. Find the values of the following :

(*i*) $\underset{x\to 0}{Lt}\ \dfrac{x-\sin x}{x^3}$. (*ii*) $\underset{x\to 0}{Lt}\ \dfrac{1-\cos x}{x^2}$.

(*iii*) $\underset{x\to 0}{Lt}\ \dfrac{\tan 2x - 2\tan x}{2x}$.

32. Find θ, when

(*i*) $\dfrac{\sin\theta}{\theta}=\dfrac{2165}{2166}$. (*ii*) $\tan\theta=\dfrac{1}{5}$. (*iii*) $\dfrac{\tan\theta}{\theta}=\dfrac{1001}{1000}$.

Answers

1. (*i*) 1. (*ii*) $-\sin 6\theta - i\cos 6\theta$. (*iii*) $\cos 13\theta + i\sin 13\theta$.

(*iv*) $2^{n+1}\sin^n\frac{1}{2}(\alpha-\beta)\cos\frac{1}{2}n(\pi+\alpha+\beta)$. (*v*) -1.

(*vi*) $2^n\cos^n\frac{1}{2}\theta\,(\cos\frac{1}{2}n\theta + i\sin\frac{1}{2}n\theta)$. (*vii*) $\cos n\theta + i\sin n\theta$.

(*viii*) $\cos 5\theta + i\sin 5\theta$.

2. (*i*) $1, \frac{1}{2}(-1\pm i\sqrt{3})$. (*ii*) $\pm 2, 2(\pm\frac{1}{2}\pm i\frac{1}{2}\sqrt{3})$.

(*iii*) $\cos\frac{1}{4}(2n\pi+\frac{3}{2}\pi) + i\sin\frac{1}{4}(2n\pi+\frac{3}{2}\pi)$, $n=0, 1, 2, 3$.

(*iv*) $\cos\frac{1}{5}(2k\pi+\frac{9}{2}\pi) + i\sin\frac{1}{5}(2k\pi+\frac{9}{2}\pi)$, $k=0, 1, 2, 3, 4$.

(*v*) $8(1+i)$. (*vi*) $\dfrac{3}{5^{\frac{3}{2}}}(\cos 3\theta - i\sin 3\theta)$, where $\theta=\tan^{-1}\frac{1}{2}$.

(*vii*) $2^{\frac{1}{7}}\{\cos\frac{1}{7}(2k\pi+\frac{1}{6}\pi) - i\sin\frac{1}{7}(2k\pi+\frac{1}{6}\pi)\}$, $k=0, 1, 2, 3, 4, 5, 6$.

(*viii*) $\dfrac{\sqrt{3}+i}{\sqrt{2}}, -\dfrac{\sqrt{3}+i}{\sqrt{2}}$.

(*ix*) $\sqrt{2}\,\{\cos\frac{1}{6}(2k+1)\pi + i\sin\frac{1}{6}(2k+1)\pi\}$, $k=0, 1, 2, 3, 4, 5$.

3. (*a*) $P=\cos\frac{5}{12}\pi + i\sin\frac{5}{12}\pi$.

$$P^{\frac{1}{4}}=\cos\frac{1}{4}\left(2k\pi+\frac{5\pi}{12}\right)+i\sin\frac{1}{4}\left(2k\pi+\frac{5\pi}{12}\right),\quad k=0, 1, 2, 3.$$

(*b*) $P=2^7\left(\cos\frac{1}{12}\pi + i\sin\frac{1}{12}\pi\right)$.

$$P^{\frac{1}{7}}=2\left\{\cos\frac{1}{7}\left(2k\pi+\frac{\pi}{12}\right)+i\sin\frac{1}{7}\left(2k\pi+\frac{\pi}{12}\right)\right\},\quad k=0, 1, 2, 3, 4, 5, 6.$$

6. (*i*) $\cos\frac{2}{5}k\pi + i\sin\frac{2}{5}k\pi$, $k=0,1,2,3,4$.

(*ii*) $a\left\{\cos\frac{1}{12}(2k+1)\pi + i\sin\frac{1}{12}(2k+1)\pi\right\}$, $k=0,1,2,\ldots\ldots,11$.

(*iii*) $\cos\frac{1}{3}k\pi + i\sin\frac{1}{3}k\pi$, $k=1,2,3,4,5$,

(*iv*) $\frac{1}{2}\left\{1+i\tan\frac{1}{8}(2k+1)\pi\right\}$, $k=0,1,2,3$.

(*v*) $\dfrac{2(2+\cos\frac{2}{3}k\pi + i\sin\frac{2}{3}k\pi)}{5+4\cos\frac{2}{3}k\pi}$, $k=0,1,2$.

(*vi*) $-\frac{1}{2}\left\{1+i\cot\frac{1}{12}(2k+1)\pi\right\}$, $k=0,1,2,3,4,5$.

(*vii*) $\cos\frac{2}{5}k\pi + i\sin\frac{2}{5}k\pi$, $k=0,1,2,3,4$

and $\cos\frac{1}{3}(2k'+1)\pi + i\sin\frac{1}{3}(2k'+1)\pi$, $k'=0,1,2$.

(*viii*) $i\tan\dfrac{k\pi}{n}$, $k=0,1,2,\ldots\ldots,(n-1)$ when n is odd and

$k=0,1,2,\ldots\ldots,(\frac{1}{2}n-1),(\frac{1}{2}n+1),\ldots\ldots,(n-1)$ when n is even.

7. $-\frac{1}{2}\left(1+i\cot\dfrac{k\pi}{n}\right)$, $k=1,2,\ldots\ldots,(n-1)$.

9. (*i*) $(x+1)(x^2-2x\cos\frac{1}{5}\pi+1)(x^2-2x\cos\frac{3}{5}\pi+1)$.

(*ii*) $\displaystyle\prod_{k=0}^{n-1}\left\{x^2-2x\cos\frac{(2k+1)\pi}{2n}+1\right\}$.

(*iii*) $\displaystyle(x+1)\prod_{k=0}^{\frac{1}{2}(n-3)}\left\{x^2-2x\cos\frac{(2k+1)\pi}{n}+1\right\}$.

10. (*i*) $\dfrac{2k\pi}{n^2}$. (*ii*) $\dfrac{(4k-1)\pi}{n(n+1)}$. 19. $-\dfrac{\pi}{3}$. 22. $(259)^2+(286)^2$.

24. (*a*) $x^2-2x\cos n\theta+1=0$. (*b*) $x^2-2^{n+1}x\cos\frac{1}{3}n\pi+2^{2n}=0$.

25. (*b*) $2\cos\frac{3}{7}\pi, 2\cos\frac{5}{7}\pi$. 26. (*b*) $8x^3+4x^2-4x-1=0$.

28. (*a*) $4\cos^3\theta-3\cos\theta$, $3\sin\theta-4\sin^3\theta$.

(*b*) (*i*) $7\sin\theta-56\sin^3\theta+112\sin^5\theta-64\sin^7\theta$.

(*ii*) $16\cos^5\theta-20\cos^3\theta+5\cos\theta$.

(*iii*) $\dfrac{5\tan\theta-10\tan^3\theta+\tan^5\theta}{1-10\tan^2\theta+5\tan^4\theta}$.

29. (*a*) $\frac{1}{2^4}\cos 5\theta + \frac{5}{2^4}\cos 3\theta + \frac{5}{2^3}\cos\theta$;

$\frac{1}{2^5}\cos 6\theta + \frac{3}{2^4}\cos 4\theta + \frac{15}{2^5}\cos 2\theta + \frac{5}{2^4}$.

(*b*) $\frac{1}{2^4}\sin 5\theta - \frac{5}{2^4}\sin 3\theta + \frac{5}{2^3}\sin\theta$;

$-\frac{1}{2^6}(\sin 7\theta - 7\sin 5\theta + 21\sin 3\theta - 35\sin\theta)$.

31. (*i*) $\frac{1}{6}$. (*ii*) $\frac{1}{2}$. (*iii*) 0 .

32. (*i*) 3° (nearly). (*ii*) $\frac{1}{16}\pi$ (nearly). (*iii*) $\frac{1}{57}\pi$ (nearly).

1.12. Definitions of exponential and trigonometrical functions of a complex variable z.

When z is complex, we define

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots\cdots ,$$

$$\sin z = z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots\cdots , \quad \cos z = 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \cdots\cdots ,$$

$$\tan z = \frac{\sin z}{\cos z} , \quad \cot z = \frac{\cos z}{\sin z} , \quad \operatorname{cosec} z = \frac{1}{\sin z} , \quad \sec z = \frac{1}{\cos z} .$$

Cor. As in the case of real index, e^z is easily found to obey the laws of indices.

We have $e^{z_1} = 1 + z_1 + \frac{z_1^2}{2!} + \frac{z_1^3}{3!} + \cdots\cdots$

and $e^{z_2} = 1 + z_2 + \frac{z_2^2}{2!} + \frac{z_2^3}{3!} + \cdots\cdots$.

Hence, by multiplication, we have

$$e^{z_1} \cdot e^{z_2} = 1 + (z_1 + z_2) + \left(\frac{z_1^2}{2!} + z_1 z_2 + \frac{z_2^2}{2!}\right) + \cdots\cdots$$

$$\cdots\cdots + \left\{\frac{z_1^n}{n!} + \frac{z_1^{n-1} z_2}{(n-1)!} + \cdots\cdots + \frac{z_1 z_2^{n-1}}{(n-1)!} + \frac{z_2^n}{n!}\right\} + \cdots\cdots$$

$$= 1 + (z_1 + z_2) + \frac{(z_1 + z_2)^2}{2!} + \cdots\cdots + \frac{(z_1 + z_2)^n}{n!} + \cdots\cdots$$

Since the infinite series representing e^{z_1} and e^{z_2} are both absolutely convergent, the product $e^{z_1}.e^{z_2}$ is also an absolutely convergent series.

Hence, by definition, $e^{z_1}.e^{z_2} = e^{z_1+z_2}$.

Similarly, $e^{z_1}.e^{z_2}.e^{z_3}\ldots\ldots = e^{z_1+z_2+z_3+\ldots\ldots}$

and $(e^z)^n = e^{nz}$, where n is a positive integer.

Also $e^{z_1} \div e^{z_2} = e^{z_1 - z_2}$.

Note. If z be complex, then e^z, sin z or cos z are mere symbols (without any significance) to represent the series on their respective right hand sides. Some authors use the symbol exp z or $E(z)$ in place of e^z, when z is complex.

For the sake of uniformity, whether z is real or complex, we write e^z.

1.13. Exponential values of sine and cosine.

We have $e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \ldots\ldots$

Putting $z = ix$, we have

$$e^{ix} = 1 + ix + \frac{(ix)^2}{2!} + \frac{(ix)^3}{3!} + \ldots\ldots$$

$$= \left(1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \ldots\ldots\right) + i\left(x - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots\ldots\right) = \cos x + i \sin x.$$

Similarly, $e^{-ix} = \cos x - i \sin x$.

Thus we have

$e^{ix} = \cos x + i \sin x$ and $e^{-ix} = \cos x - i \sin x$.

Also, by addition and subtraction, we have

$$\cos x = \frac{1}{2}(e^{ix} + e^{-ix}) \text{ and } \sin x = \frac{1}{2i}(e^{ix} - e^{-ix}).$$

These expressions are known as *Euler's exponential values* of cos x and sin x.

Cor. Since $(e^{i\theta})^n = e^{in\theta}$, where θ is real or complex, we have

$$(\cos\theta + i \sin\theta)^n = \cos n\theta + i \sin n\theta.$$

Thus De Moivre's theorem holds good, whether θ is real or complex.

1.14. Some properties of sine and cosine.

(*a*) By definition, we have

$$\cos(-x) = \frac{1}{2}\{e^{i(-x)} + e^{-i(-x)}\} = \frac{1}{2}(e^{-ix} + e^{ix}) = \cos x$$

and $$\sin(-x) = \frac{1}{2i}\{e^{i(-x)} - e^{-i(-x)}\} = \frac{1}{2i}(e^{-ix} - e^{ix}) = -\sin x.$$

(*b*) We have, from the definitions of $\sin x$ and $\cos x$,

$$\sin^2 x + \cos^2 x = \left\{\frac{1}{2i}(e^{ix} - e^{-ix})\right\}^2 + \left\{\frac{1}{2}(e^{ix} + e^{-ix})\right\}^2$$

$$= \frac{1}{4}\{(e^{ix} + e^{-ix})^2 - (e^{ix} - e^{-ix})^2\}$$

$$= \frac{1}{4} \cdot 4 \cdot e^{ix} \cdot e^{-ix} = 1.$$

(*c*) From the definitions, we have

$$\sin x \cos y + \cos x \sin y$$

$$= \frac{1}{2i}(e^{ix} - e^{-ix}) \cdot \frac{1}{2}(e^{iy} + e^{-iy}) + \frac{1}{2}(e^{ix} + e^{-ix}) \frac{1}{2i}(e^{iy} - e^{-iy})$$

$$= \frac{1}{4i}(e^{ix} \cdot 2e^{iy} - e^{-ix} \cdot 2e^{-iy}) = \frac{1}{2i}\{e^{i(x+y)} - e^{-i(x+y)}\}$$

$$= \sin(x+y).$$

Similarly, we have

$$\sin(x-y) = \sin x \cos y - \cos x \sin y,$$

$$\cos(x+y) = \cos x \cos y - \sin x \sin y$$

and $$\cos(x-y) = \cos x \cos y + \sin x \sin y.$$

(*d*) We have, from the definitions of $\sin x$ and $\cos x$,

$$2 \sin x \cos x = 2 \cdot \frac{1}{2i}(e^{ix} - e^{-ix}) \cdot \frac{1}{2}(e^{ix} + e^{-ix})$$

$$= \frac{1}{2i}(e^{2ix} - e^{-2ix}) = \sin 2x.$$

Similarly, we have

$$\cos 2x = \cos^2 x - \sin^2 x = 2\cos^2 x - 1 = 1 - 2\sin^2 x.$$

Putting simply $y = x$ in the formulae of $\sin(x+y)$ and $\cos(x+y)$, we may have the above formulae of $\sin 2x$ and $\cos 2x$ also.

Note. It may be shown that, if x be complex, then $\sin x$, $\cos x$, $\tan x$, etc. also satisfy all the relations of trigonometric functions of a real variable.

1.15. Periods of trigonometrical and exponential functions.

If $f(x+\mu)=f(x)$ for all values of x, then $f(x)$ is called a *periodic function of x of period μ*. It follows that, if m be any integer, positive or negative, and $f(x)$ be a periodic function of x of period μ, then

$$f(x+m\mu)=f(x).$$

If n be any integer and x be real or complex, then we have

$$\sin(2n\pi+x)=\sin 2n\pi\cos x+\cos 2n\pi\sin x$$
$$=0.\cos x+1.\sin x=\sin x.$$

Hence, even when x is complex, $\sin x$ is a periodic function of x.

Similarly, $\cos x$ also is a periodic function of x.

Again $\tan(n\pi+x)=\tan x$.

Therefore $\tan x$ is also a periodic function of x.

Also $e^{2n\pi i+x}=e^{2n\pi i}.e^{x}=(\cos 2n\pi+i\sin 2n\pi)e^{x}=e^{x}$.

Therefore e^{x} is a periodic function of x.

Again $e^{i(2n\pi+x)}=\cos(2n\pi+x)+i\sin(2n\pi+x)$

$$=\cos x+i\sin x=e^{ix}.$$

Therefore e^{ix} is also a periodic function of x.

Note. As in the case of real values of x, the periods of $\sin x$, $\cos x$ and $\tan x$, (x being complex), are 2π, 2π and π respectively.

1.16. Logarithm of a complex number.

If the two complex numbers z and $N(\neq 0)$ be such that $e^{z}=N$, then z is defined to be the *logarithm* of N.

If n be zero or any integer, then we have

$$e^{2n\pi i}=\cos 2n\pi+i\sin 2n\pi=1.$$

So we can write $N=e^{z}=e^{z}.e^{2n\pi i}=e^{z+2n\pi i}$

Hence $(z+2n\pi i)$ is also the logarithm of N and we write $\text{Log}\,N=z+2n\pi i$. Since n may have an infinite number of values, we see that logarithm of a complex quantity is a multi-valued function. When $n=0$, we write $\log N=z$. This is called the *principal value* of the logarithm. Thus we have $\text{Log}\,N=\log N+2n\pi i$.

Writing the complex number z in polar form, we have

$$z = r(\cos\theta + i\sin\theta) = re^{i\theta},$$

where $r = |z|$ and $\theta = \text{amp } z$, $(-\pi < \theta \leq \pi)$.

Then $\text{Log } z = \log r + i(\theta + 2n\pi) = \log|z| + i(\text{amp } z + 2n\pi)$.

Taking the principal value, we have $\log z = \log|z| + i \text{ amp } z$.

Cor. As in the case of real variable, it may be proved that

$$\log(1+z) = z - \tfrac{1}{2}z^2 + \tfrac{1}{3}z^3 - \ldots\ldots,$$

where z is a complex number and $|z| < 1$.

Thus $\text{Log}(1+z) = 2n\pi i + \log(1+z) = 2n\pi i + z - \tfrac{1}{2}z^2 + \tfrac{1}{3}z^3 - \ldots\ldots,$ if $|z| < 1$.

When $|z| = 1$, the expansion is valid, if amp z be not equal to an odd multiple of π.

Note. When the multi-valuedness of a function is taken into account, the function is written with a capital letter to distinguish it from its principal value.

1.17. Properties of logarithms.

(*a*) *For the non-zero complex numbers x and y,*

$$\text{Log}(xy) = \text{Log } x + \text{Log } y.$$

Let $x = e^{z_1}$ and $y = e^{z_2}$. Therefore $xy = e^{z_1} \cdot e^{z_2} = e^{z_1 + z_2}$.

By definition, $\text{Log } x = z_1 + 2n_1\pi i$, $\text{Log } y = z_2 + 2n_2\pi i$ and $\text{Log}(xy) = z_1 + z_2 + 2n_3\pi i$, where n_1, n_2 and n_3 are integers.

Therefore $\text{Log } x + \text{Log } y = z_1 + z_2 + 2(n_1 + n_2)\pi i$

$$= z_1 + z_2 + 2n_3\pi i = \text{Log}(xy),$$

where we take $n_3 = n_1 + n_2 =$ an integer.

Note. In general, $\log(xy) \neq \log x + \log y$.

For example, if $x = -1$ and $y = i$, then $\log(xy) = \log(-i) = -\tfrac{1}{2}\pi i$, $\log x = \pi i$ and $\log y = \tfrac{1}{2}\pi i$; therefore $\log(xy) \neq \log x + \log y$.

(*b*) *For the non-zero complex numbers x and y,*

$$\text{Log}\frac{x}{y} = \text{Log } x - \text{Log } y.$$

Let $x = e^{z_1}$ and $y = e^{z_2}$. Therefore $\frac{x}{y} = \frac{e^{z_1}}{e^{z_2}} = e^{z_1 - z_2}$.

By definition, $\text{Log } x = z_1 + 2n_1 \pi i$, $\text{Log } y = z_2 + 2n_2 \pi i$ and $\text{Log } \frac{x}{y} = z_1 - z_2 + 2n_3 \pi i$, where n_1, n_2 and n_3 are integers.

Therefore $\text{Log } x - \text{Log } y = z_1 - z_2 + 2(n_1 - n_2)\pi i$

$$= z_1 - z_2 + 2n_3 \pi i = \text{Log } \frac{x}{y},$$

where we take $n_3 = n_1 - n_2 =$ an integer.

Note. In general, $\log \frac{x}{y} \neq \log x - \log y$.

For example, if $x = -1$ and $y = -i$, then $\log \frac{x}{y} \neq \log x - \log y$.

(*c*) In the same way, it may be proved that

$$\text{Log } x^y = y \text{ Log } x + 2n\pi i,$$

where $x (\neq 0)$, y *are two complex numbers and* $n = 0$ *or any integer.*

(*d*) Logarithm of a negative number $(-x)$ is given by

$$\text{Log } (-x) = \text{Log } \{(-1).x\}$$

$$= \text{Log } \left\{e^{(2n+1)\pi i}.x\right\} = \log x + (2n+1)\pi i$$

and $$\log (-x) = \log x + \pi i.$$

Thus $\text{Log } (-e) = \log e + (2n+1)\pi i = 1 + (2n+1)\pi i.$

1.18. Definition of a^z.

If $a (\neq 0)$ and z be two complex numbers, we define a^z as $a^z = e^{z \text{Log } a} = e^{z(\log a + 2n\pi i)}$, where $n = 0$ or any integer.

Thus a^z is also a multi-valued function.

Taking $n = 0$, we have the principal value of a^z as $e^{z \log a}$.

In this case,

$$a^z = 1 + z \log a + \frac{1}{2!}(z \log a)^2 + \frac{1}{3!}(z \log a)^3 + \cdots\cdots$$

Putting $z = 1$, we get

$$a = 1 + \log a + \frac{(\log a)^2}{2!} + \frac{(\log a)^3}{3!} + \cdots\cdots$$

1.19. Inverse circular functions.

If $\cos(x+iy)=a+ib$, we then define $x+iy$ as an inverse cosine of $(a+ib)$ and we write it as $\mathrm{Cos}^{-1}(a+ib)$. Since cosine function is periodic, we have, for all integral values of n,

$$\cos(x+iy)=\cos\{2n\pi\pm(x+iy)\}=a+ib.$$

Therefore $\mathrm{Cos}^{-1}(a+ib)=2n\pi\pm(x+iy)$.

Since n may have an infinite number of values, it is a multi-valued function. Its principal value is obtained by simply putting $n=0$ and is written as $\cos^{-1}(a+ib)$. The real part of the principal value lies in $(0,\pi)$.

Thus $\mathrm{Cos}^{-1}(a+ib)=2n\pi+\cos^{-1}(a+ib)$.

If we take $z=x+iy$ and $w=a+ib$ such that $\cos z=w$, then

$$\sin z=\pm\sqrt{1-w^2} \quad \text{and} \quad e^{iz}=w\pm i\sqrt{1-w^2}.$$

Hence $z=\mathrm{Cos}^{-1}w=-i\,\mathrm{Log}\,(w\pm i\sqrt{1-w^2})$,

whose principal value is obtained by choosing $\sin z=+\sqrt{1-w^2}$ and taking the principal value of the logarithm.

Similarly, if $\sin(x+iy)=a+ib$, we may write

$$a+ib=\sin\{n\pi+(-1)^n(x+iy)\},$$

so that $\mathrm{Sin}^{-1}(a+ib)=n\pi+(-1)^n(x+iy)$

$$=n\pi+(-1)^n\sin^{-1}(a+ib).$$

Its principal value is obtained by putting $n=0$.

The real part of the principal value lies in $(-\frac{1}{2}\pi,\frac{1}{2}\pi)$.

Taking $z=x+iy$ and $w=a+ib$ such that $\sin z=w$, we have

$$z=\mathrm{Sin}^{-1}w=-i\,\mathrm{Log}\,(iw\pm\sqrt{1-w^2}).$$

Similarly, $\mathrm{Tan}^{-1}(a+ib)=n\pi+\tan^{-1}(a+ib)$.

The real part of the principal value lies in $(-\frac{1}{2}\pi,\frac{1}{2}\pi)$.

If we take $z=x+iy$ and $w=a+ib$ such that $\tan z=w$, then

$$\frac{e^{iz}-e^{-iz}}{i(e^{iz}+e^{-iz})}=w$$

or, $e^{2iz}(1-wi)=1+wi$, giving $e^{2iz}=\dfrac{1+wi}{1-wi}$, if $wi\neq 1$.

Hence $z = \text{Tan}^{-1} w = -\frac{i}{2}\text{Log}\frac{1+wi}{1-wi}$.

Similarly, other inverse circular functions are defined.

1.20. Gregory's series.

To expand θ *in powers of* $\tan\theta$.

We have $i\tan\theta = \frac{i\sin\theta}{\cos\theta}$.

Applying componendo and dividendo, we get

$$\frac{1+i\tan\theta}{1-i\tan\theta} = \frac{\cos\theta+i\sin\theta}{\cos\theta-i\sin\theta} = \frac{e^{i\theta}}{e^{-i\theta}} = e^{2i\theta}.$$

Considering the principal values of the logarithms of both sides, we have

$$\begin{aligned} 2i\theta &= \log(1+i\tan\theta) - \log(1-i\tan\theta) \\ &= (i\tan\theta - \tfrac{1}{2}i^2\tan^2\theta + \tfrac{1}{3}i^3\tan^3\theta - \dots\dots) \\ &\qquad -(-i\tan\theta - \tfrac{1}{2}i^2\tan^2\theta - \tfrac{1}{3}i^3\tan^3\theta - \dots\dots) \\ &= 2i(\tan\theta - \tfrac{1}{3}\tan^3\theta + \tfrac{1}{5}\tan^5\theta - \dots\dots) \end{aligned}$$

or, $\theta = \tan\theta - \frac{1}{3}\tan^3\theta + \frac{1}{5}\tan^5\theta - \dots\dots$ to infinity.

This is called *Gregory's series*, named after its discoverer, Prof. James Gregory and this is valid when

$$|\tan\theta| \le 1, \text{ that is, } -\tfrac{1}{4}\pi \le \theta \le \tfrac{1}{4}\pi.$$

Putting $\tan\theta = x$, so that $\theta = \tan^{-1}x$, the above series may be written as $\tan^{-1}x = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \dots\dots + (-1)^{n-1}\frac{x^{2n-1}}{2n-1} + \dots\dots$, where $-1 \le x \le 1$ and $\tan^{-1}x$ has its principal value.

Note 1. If the general values of the logarithms be considered, then

$$\theta - n\pi = \tan\theta - \tfrac{1}{3}\tan^3\theta + \tfrac{1}{5}\tan^5\theta - \dots\dots, \text{ provided } -\tfrac{1}{4}\pi \le \theta \le \tfrac{1}{4}\pi.$$

Note 2. Putting $\theta = \frac{1}{4}\pi$ in Gregory's series, we have $\pi = 4(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \dots)$, which may be used to calculate the value of π.

1.21. Hyperbolic functions.

Hyperbolic functions are defined as below :

Hyperbolic sine : $\sinh x = \frac{1}{2}(e^x - e^{-x})$;

Hyperbolic cosine : $\cosh x = \frac{1}{2}(e^x + e^{-x})$.

Also $\tanh x = \dfrac{\sinh x}{\cosh x}$, $\operatorname{cosech} x = \dfrac{1}{\sinh x}$,

$\operatorname{sech} x = \dfrac{1}{\cosh x}$, $\coth x = \dfrac{1}{\tanh x}$.

From the definitions, it follows that

$$e^x = \cosh x + \sinh x \text{ and } e^{-x} = \cosh x - \sinh x;$$

$\sinh x$ is an increasing function of x and $\cosh x \geq 1$ for all real values of x.

We have $\sin(ix) = \dfrac{e^{i(ix)} - e^{-i(ix)}}{2i} = \dfrac{e^{-x} - e^{x}}{2i^2} i$

$$= \tfrac{1}{2} i (e^x - e^{-x}) = i \sinh x$$

and $\cos(ix) = \dfrac{e^{i(ix)} + e^{-i(ix)}}{2} = \dfrac{e^{-x} + e^{x}}{2} = \cosh x.$

Similarly, $\tan(ix) = i \tanh x$.

Again $\sinh x = \dfrac{\sin(ix)}{i} = -i \sin(ix)$

and $\cosh x = \cos(ix)$.

Expanding e^x and e^{-x}, we get the expansions of $\sinh x$ and $\cosh x$ as

$$\sinh x = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots\ldots$$

and

$$\cosh x = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \ldots\ldots$$

The hyperbolic functions have similar formulae as those of trigonometric functions of a complex variable. These formulae can be deduced directly from the definitions.

Some of these formulae are

(*i*) $\sinh(-x) = -\sinh x$, $\cosh(-x) = \cosh x$,

$\sinh 0 = 0$, $\cosh 0 = 1$, $\tanh 0 = 0$.

(*ii*) $\cosh^2 x - \sinh^2 x = 1 = \operatorname{sech}^2 x + \tanh^2 x = \coth^2 x - \operatorname{cosech}^2 x$.

(*iii*) $\sinh(x \pm y) = \sinh x \cosh y \pm \cosh x \sinh y$;

$\cosh(x \pm y) = \cosh x \cosh y \pm \sinh x \sinh y$;

$$\tanh(x \pm y) = \frac{\tanh x \pm \tanh y}{1 \pm \tanh x \tanh y}.$$

(*iv*) $\sinh(2x) = 2\sinh x \cosh x$;

$\cosh(2x) = \cosh^2 x + \sinh^2 x$

$= 2\cosh^2 x - 1 = 1 + 2\sinh^2 x$;

$\tanh(2x) = \dfrac{2\tanh x}{1+\tanh^2 x}$.

(*v*) $\sinh x + \sinh y = 2\sinh \frac{1}{2}(x+y)\cosh \frac{1}{2}(x-y)$;

$\sinh x - \sinh y = 2\cosh \frac{1}{2}(x+y)\sinh \frac{1}{2}(x-y)$;

$\cosh x + \cosh y = 2\cosh \frac{1}{2}(x+y)\cosh \frac{1}{2}(x-y)$;

$\cosh x - \cosh y = 2\sinh \frac{1}{2}(x+y)\sinh \frac{1}{2}(x-y)$.

(*vi*) $2\sinh x \cosh y = \sinh(x+y) + \sinh(x-y)$;

$2\cosh x \sinh y = \sinh(x+y) - \sinh(x-y)$;

$2\cosh x \cosh y = \cosh(x+y) + \cosh(x-y)$;

$2\sinh x \sinh y = \cosh(x+y) - \cosh(x-y)$.

(*vii*) $\sinh(2n\pi i + x) = \sinh x$; $\cosh(2n\pi i + x) = \cosh x$;

$\tanh(n\pi i + x) = \tanh x$, where $n = 0$ or any integer.

Thus $\sinh x$, $\cosh x$ and $\tanh x$ are periodic functions of imaginary periods.

(*viii*) If $\sinh x = \omega$ then $\sinh^{-1}\omega = x$; if $\cosh x = \omega$, then $\cosh^{-1}\omega = x$ and if $\tanh x = \omega$, then $\tanh^{-1}\omega = x$.

(*ix*) $\sinh^{-1} x = -i\sin^{-1}(ix)$;

$\cosh^{-1} x = -i\cos^{-1} x$;

$\tanh^{-1} x = -i\tan^{-1}(ix)$.

Note. The hyperbolic sine and cosine are related to a rectangular hyperbola $x^2 - y^2 = a^2$ in the same way as the trigonometric sine and cosine to the circle $x^2 + y^2 = a^2$. This is why the former are called *hyperbolic functions* and the latter are called *circular functions*.

1.22. Illustrative Examples.

Ex. 1. *If x and y be complex, then prove, from the definitions of sine and cosine of complex numbers, that*

$$\cos x - \cos y = 2\sin \tfrac{1}{2}(y+x)\sin \tfrac{1}{2}(y-x).$$

From definitions, we have

$$2\sin\tfrac{1}{2}(y+x)\sin\tfrac{1}{2}(y-x)$$

$$=2.\frac{1}{2i}\left\{e^{\frac{i}{2}(y+x)}-e^{-\frac{i}{2}(y+x)}\right\}\frac{1}{2i}\left\{e^{\frac{i}{2}(y-x)}-e^{-\frac{i}{2}(y-x)}\right\}$$

$$=-\frac{1}{2}\left\{e^{\frac{i}{2}(y+x+y-x)}-e^{\frac{i}{2}(y+x-y+x)}-e^{\frac{i}{2}(-y-x+y-x)}+e^{-\frac{i}{2}(y+x+y-x)}\right\}$$

$$=-\frac{1}{2}(e^{iy}-e^{ix}-e^{-ix}+e^{-iy})=\frac{1}{2}(e^{ix}+e^{-ix})-\frac{1}{2}(e^{iy}+e^{-iy})=\cos x-\cos y.$$

Ex. 2. *Find the general value of* i^i. [*B. H. 1966 ; K. H. 2003*]

We have $e^{i\frac{\pi}{2}}=\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}=i$.

Therefore $\operatorname{Log} i=2n\pi i+i\frac{\pi}{2}$, where n is any integer.

Hence $i^i=e^{i\operatorname{Log} i}=e^{i(2n\pi+\frac{\pi}{2})i}=e^{-(2n+\frac{1}{2})\pi}$.

Ex. 3. *If m and n be real, then show that*

$$\operatorname{Log}(m+in)=\tfrac{1}{2}\log(m^2+n^2)+i\left(2k\pi+\tan^{-1}\frac{n}{m}\right),$$

k being any integer. [*T. H. 2008*]

Let $m=r\cos\theta$ and $n=r\sin\theta$, so that $r^2=m^2+n^2$ and $\tan\theta=\frac{n}{m}$.

Therefore $m+in=r(\cos\theta+i\sin\theta)=re^{i\theta}=re^{i(2k\pi+\theta)}$, where k is an integer.

Hence $\operatorname{Log}(m+in)=\log r+i(2k\pi+\theta)$

$$=\log(m^2+n^2)^{\frac{1}{2}}+i\left(2k\pi+\tan^{-1}\frac{n}{m}\right)$$

$$=\frac{1}{2}\log(m^2+n^2)+i\left(2k\pi+\tan^{-1}\frac{n}{m}\right).$$

Ex. 4. *Express $(a+ib)^{p+iq}$ in the form $(A+iB)$, where a, b, p, q are real quantities.*

We have $(a+ib)^{p+iq}=e^{(p+iq)\operatorname{Log}(a+ib)}$

$$=e^{(p+iq)\left\{\frac{1}{2}\log(a^2+b^2)+i\left(2k\pi+\tan^{-1}\frac{b}{a}\right)\right\}},$$

by the previous Ex. 3

$$=e^{P+iQ},$$

where $P=\frac{p}{2}\log(a^2+b^2)-q\left(2k\pi+\tan^{-1}\frac{b}{a}\right)$

and $Q=\frac{q}{2}\log(a^2+b^2)+p\left(2k\pi+\tan^{-1}\frac{b}{a}\right)$.

Hence $(a+ib)^{p+iq}=e^P.e^{iQ}=e^P(\cos Q+i\sin Q)=e^P\cos Q+ie^P\sin Q$.

Ex. 5. *Find the general values and the principal value of* $(-1+i)^i$. [*C. H. 1987*]

We have $-1+i=\sqrt{2}\left(\cos\frac{3}{4}\pi+i\sin\frac{3}{4}\pi\right)$.

Therefore $\text{Log}(-1+i)=\frac{1}{2}\log 2+i\left(2k\pi+\frac{3}{4}\pi\right)$, where k is an integer.

Hence $(-1+i)^i=e^{i\,\text{Log}(-1+i)}=e^{-\left(2k\pi+\frac{3}{4}\pi\right)+i.\frac{1}{2}\log 2}$

$$=e^{-\left(2k+\frac{3}{4}\right)\pi}\left\{\cos\left(\tfrac{1}{2}\log 2\right)+i\sin\left(\tfrac{1}{2}\log 2\right)\right\}.$$

Its principal value is $e^{-\frac{3}{4}\pi}\left\{\cos\left(\frac{1}{2}\log 2\right)+i\sin\left(\frac{1}{2}\log 2\right)\right\}$, which is obtained by putting $k=0$.

Ex. 6. (*a*) *Separate* $\sin(x+iy)$ *into real and imaginary parts,* x *and* y *being real.*

Also show that $|\sin(x+iy)|^2=\sin^2 x+\frac{1}{4}(e^y-e^{-y})^2$. [*C. H. 1969*]

(*b*) *Express* $\sinh(x+iy)$ *in the form* $(A+iB)$. [*V. H. 2002*]

(*a*) We have

$$\sin(x+iy)=\frac{1}{2i}\left\{e^{i(x+iy)}-e^{-i(x+iy)}\right\}=\frac{1}{2i}\left\{e^{ix}.e^{-y}-e^{-ix}.e^{y}\right\}$$

$$=\frac{e^{-y}}{2i}(\cos x+i\sin x)-\frac{e^{y}}{2i}(\cos x-i\sin x)$$

$$=\tfrac{1}{2}e^{-y}(\sin x-i\cos x)+\tfrac{1}{2}e^{y}(\sin x+i\cos x)$$

$$=\tfrac{1}{2}(e^{y}+e^{-y})\sin x+i.\tfrac{1}{2}(e^{y}-e^{-y})\cos x.$$

Hence the real part is $\frac{1}{2}(e^y+e^{-y})\sin x$ and the imaginary part is

$$\tfrac{1}{2}(e^{y}-e^{-y})\cos x.$$

Therefore $|\sin(x+iy)|^2=\frac{1}{4}(e^y+e^{-y})^2\sin^2 x+\frac{1}{4}(e^y-e^{-y})^2\cos^2 x$

$$=\tfrac{1}{4}(e^{y}+e^{-y})^2\sin^2 x+\tfrac{1}{4}(e^{y}-e^{-y})^2(1-\sin^2 x)$$

$$=\tfrac{1}{4}\sin^2 x\left\{(e^{y}+e^{-y})^2-(e^{y}-e^{-y})^2\right\}+\tfrac{1}{4}(e^{y}-e^{-y})^2$$

$$=\tfrac{1}{4}\sin^2 x.4e^{y}.e^{-y}+\tfrac{1}{4}(e^{y}-e^{-y})^2$$

$$=\sin^2 x+\tfrac{1}{4}(e^{y}-e^{-y})^2.$$

(*b*) $\sinh(x+iy) = -i\sin\{i(x+iy)\}$

$= -i\sin(ix-y)$

$= -i\{\sin(ix)\cos y - \cos(ix)\sin y\}$

$= -i(i\sinh x\cos y - \cosh x\sin y)$

$= \sinh x\cos y + i\cosh x\sin y.$

Ex. 7. *Prove that* $\mathrm{Sin}^{-1}\sqrt{-1} = n\pi + (-1)^n i\log(\sqrt{2}+1)$, *where* n *is any integer.*

Let $\mathrm{Sin}^{-1}\sqrt{-1} = \theta$, so that $\sin\theta = \sqrt{-1}$ and $\cos\theta = \sqrt{1-\sin^2\theta} = \pm\sqrt{2}$.

Hence $e^{i\theta} = \cos\theta + i\sin\theta = \pm\sqrt{2} + i\sqrt{-1} = \pm\sqrt{2} - 1.$

When $e^{i\theta} = \sqrt{2} - 1$, then

$i\theta = \mathrm{Log}(\sqrt{2}-1) = 2m\pi i + \log(\sqrt{2}-1)$, where m is an integer.

Therefore $\theta = 2m\pi - i\log(\sqrt{2}-1) = 2m\pi + i\log(\sqrt{2}+1)$. ... (1)

When $e^{i\theta} = -\sqrt{2} - 1$, then

$i\theta = \mathrm{Log}(-\sqrt{2}-1) = 2m\pi i + \pi i + \log(\sqrt{2}+1).$

Therefore $\theta = (2m+1)\pi - i\log(\sqrt{2}+1)$. ... (2)

Combining (1) and (2), we get the result.

Ex. 8. *Find a complex number* z *such that* (*i*) $e^z = i$, (*ii*) $\cosh z = \frac{1}{2}$.

(*i*) We have $e^z = i = \cos\frac{1}{2}\pi + i\sin\frac{1}{2}\pi = e^{i\frac{\pi}{2}} = e^{i(2n\pi+\frac{\pi}{2})}$, where n is any integer.

Therefore $z = i(2n+\frac{1}{2})\pi$.

(*ii*) Here $\cosh z = \frac{1}{2}\left(e^z + e^{-z}\right) = \frac{1}{2}$

or, $\left(e^z\right)^2 - e^z + 1 = 0$

or, $e^z = \frac{1}{2}(1 \pm i\sqrt{3}) = \cos\frac{1}{3}\pi \pm i\sin\frac{1}{3}\pi = e^{\pm\frac{1}{3}\pi i}$

$= e^{(2n\pm\frac{1}{3})\pi i}$, where n is any integer.

Therefore $z = i(2n\pm\frac{1}{3})\pi$.

Ex. 9. *Prove that* $\sin\left(i\log\dfrac{a-ib}{a+ib}\right) = \dfrac{2ab}{a^2+b^2}$. [*C. H. 2001*]

Let $a = r\cos\theta$ and $b = r\sin\theta$, so that $\tan\theta = \dfrac{b}{a}$.

Therefore $\dfrac{a-ib}{a+ib} = \dfrac{r(\cos\theta - i\sin\theta)}{r(\cos\theta + i\sin\theta)} = \dfrac{e^{-i\theta}}{e^{i\theta}} = e^{-2i\theta}$.

Therefore $\log \dfrac{a-ib}{a+ib} = -2i\theta$.

Hence $\sin\left(i \log \dfrac{a-ib}{a+ib}\right) = \sin\{i(-2i\theta)\} = \sin 2\theta$

$$= \frac{2\tan\theta}{1+\tan^2\theta} = \frac{\dfrac{2b}{a}}{1+\dfrac{b^2}{a^2}} = \frac{2ab}{a^2+b^2}.$$

Ex. 10. *Show that the equation* $\tan\left(i \log \dfrac{x-iy}{x+iy}\right) = 2$ *represents the rectangular hyperbola* $x^2 - y^2 = xy$. [*T. H. 2009*]

Putting $x = r\cos\theta$ and $y = r\sin\theta$, whence $\tan\theta = \dfrac{y}{x}$, we get

$$\frac{x-iy}{x+iy} = \frac{r(\cos\theta - i\sin\theta)}{r(\cos\theta + i\sin\theta)} = \frac{e^{-i\theta}}{e^{i\theta}} = e^{-2i\theta}.$$

Therefore $\log \dfrac{x-iy}{x+iy} = -2i\theta$.

Hence the equation $\tan\left(i \log \dfrac{x-iy}{x+iy}\right) = 2$ gives

$$\tan\{i(-2i\theta)\} = 2$$

or, $\tan 2\theta = \dfrac{2\tan\theta}{1-\tan^2\theta} = \dfrac{\dfrac{2y}{x}}{1-\dfrac{y^2}{x^2}} = 2$, that is, $\dfrac{xy}{x^2-y^2} = 1$,

which is the rectangular hyperbola $x^2 - y^2 = xy$.

Ex. 11. *If* a, z_1, z_2 *be complex, examine the validity of the relation*

$$a^{z_1} \cdot a^{z_2} = a^{z_1+z_2}.$$ [*C. H. 1979*]

We have $a^{z_1} = e^{z_1 \operatorname{Log} a} = e^{z_1(\log a + 2n_1\pi i)}$,

$$a^{z_2} = e^{z_2 \operatorname{Log} a} = e^{z_2(\log a + 2n_2\pi i)}$$

and $a^{z_1+z_2} = e^{(z_1+z_2)\operatorname{Log} a} = e^{(z_1+z_2)(\log a + 2n_3\pi i)}$,

where n_1, n_2 and n_3 are integers.

Now $a^{z_1} \cdot a^{z_2} = e^{z_1(\log a + 2n_1\pi i) + z_2(\log a + 2n_2\pi i)}$

$$= e^{(z_1+z_2)\log a + 2(n_1 z_1 + n_2 z_2)\pi i}$$

Since n_1, n_2 and n_3 are arbitrary integers, $(n_1z_1 + n_2z_2)$ is generally not equal to $n_3(z_1+z_2)$.

Therefore, in general, $a^{z_1} \cdot a^{z_2} \neq a^{z_1+z_2}$.

Note. The principal value of $a^{z_1} \cdot a^{z_2}$ is equal to that of $a^{z_1+z_2}$.

Ex.12. *If* $u+iv=\tan(x+iy)$, *then show that* $u^2+v^2+2u\cot 2x=1$ *and* $u^2+v^2+2v\cdot\dfrac{e^{-2y}+e^{2y}}{e^{-2y}-e^{2y}}+1=0$. [*T. H. 2009*]

We have $\tan(x+iy)=u+iv$.

or, $x+iy=\tan^{-1}(u+iv)$. ... (1)

Therefore $x-iy=\tan^{-1}(u-iv)$. ... (2)

Adding (1) and (2), we get

$$2x=\tan^{-1}(u+iv)+\tan^{-1}(u-iv)$$

$$=\tan^{-1}\frac{u+iv+u-iv}{1-(u+iv)(u-iv)}=\tan^{-1}\frac{2u}{1-(u^2+v^2)}$$

or, $\dfrac{2u}{1-u^2-v^2}=\tan 2x=\dfrac{1}{\cot 2x}$

or, $2u\cot 2x=1-u^2-v^2$

or, $u^2+v^2+2u\cot 2x=1$.

Subtracting (2) from (1), we get

$$2iy=\tan^{-1}(u+iv)-\tan^{-1}(u-iv)$$

$$=\tan^{-1}\frac{(u+iv)-(u-iv)}{1+(u+iv)(u-iv)}=\tan^{-1}\frac{2iv}{1+u^2+v^2}$$

$$\text{or, } \frac{2iv}{1+u^2+v^2}=\tan 2iy=\frac{\sin 2iy}{\cos 2iy}=\frac{\frac{1}{2i}\{e^{i(2iy)}-e^{-i(2iy)}\}}{\frac{1}{2}\{e^{i(2iy)}+e^{-i(2iy)}\}}=\frac{1}{i}\cdot\frac{e^{-2y}-e^{2y}}{e^{-2y}+e^{2y}}$$

$$\text{or, } \frac{u^2+v^2+1}{2iv}=i\frac{e^{-2y}+e^{2y}}{e^{-2y}-e^{2y}}$$

$$\text{or, } u^2+v^2+1=2i^2v\,\frac{e^{-2y}+e^{2y}}{e^{-2y}-e^{2y}}=-2v\,\frac{e^{-2y}+e^{2y}}{e^{-2y}-e^{2y}}$$

$$\text{or, } u^2+v^2+2v\,\frac{e^{-2y}+e^{2y}}{e^{-2y}-e^{2y}}+1=0.$$

Ex. 13. *If* $\sin(\alpha+i\beta)=x+iy$, *then prove that*

$$\frac{x^2}{\sin^2\alpha}-\frac{y^2}{\cos^2\alpha}=1 \text{ and } \frac{x^2}{\cosh^2\beta}+\frac{y^2}{\sinh^2\beta}=1.$$

We have $x+iy=\sin(\alpha+i\beta)=\sin\alpha\cos i\beta+\cos\alpha\sin i\beta$

$=\sin\alpha\cosh\beta+i\cos\alpha\sinh\beta$. ... (1)

Also $x-iy=\sin\alpha\cosh\beta-i\cos\alpha\sinh\beta$. ... (2)

By addition and subtraction of (1) and (2), we get

$$x = \sin\alpha \cosh\beta \quad \text{and} \quad y = \cos\alpha \sinh\beta.$$

Hence $$\frac{x^2}{\sin^2\alpha} - \frac{y^2}{\cos^2\alpha} = \frac{\sin^2\alpha \cosh^2\beta}{\sin^2\alpha} - \frac{\cos^2\alpha \sinh^2\beta}{\cos^2\alpha}$$

$$= \cosh^2\beta - \sinh^2\beta = 1$$

and $$\frac{x^2}{\cosh^2\beta} + \frac{y^2}{\sinh^2\beta} = \frac{\sin^2\alpha \cosh^2\beta}{\cosh^2\beta} + \frac{\cos^2\alpha \sinh^2\beta}{\sinh^2\beta}$$

$$= \sin^2\alpha + \cos^2\alpha = 1 .$$

Ex. 14. *If* $\cosh^{-1}(x+iy) + \cosh^{-1}(x-iy) = \cosh^{-1} a$, *where* a *is a constant* > 1, *then show that* (x, y) *lies on an ellipse.* [*C. H. 1981*]

Let $\cosh^{-1}(x+iy) = u + iv$.

Therefore $x + iy = \cosh(u+iv) = \cosh u \cos v + i \sinh u \sin v$,

whence $x = \cosh u \cos v$ and $y = \sinh u \sin v$.

Again $\cosh^{-1}(x-iy) = u - iv$.

Therefore, from the given relation,

$$u + iv + u - iv = \cosh^{-1} a$$

or, $$\cosh 2u = a.$$

Now $$\frac{x^2}{\cosh^2 u} + \frac{y^2}{\sinh^2 u} = \cos^2 v + \sin^2 v = 1$$

or, $$\frac{x^2}{\frac{1}{2}(1+\cosh 2u)} + \frac{y^2}{\frac{1}{2}(\cosh 2u - 1)} = 1$$

or, $$\frac{x^2}{\frac{1}{2}(a+1)} + \frac{y^2}{\frac{1}{2}(a-1)} = 1.$$

Hence (x, y) lies on an ellipse, since $a > 1$.

Note. If $a > 1$, then the curve is an ellipse but if $a < 1$, then the curve becomes a hyperbola.

Ex. 15. *Find the sum to* n *terms of the series,* α *and* β *being real,*

$$\cos\alpha + \cos(\alpha+\beta) + \cos(\alpha+2\beta) + \cdots\cdots$$

and $$\sin\alpha + \sin(\alpha+\beta) + \sin(\alpha+2\beta) + \cdots\cdots$$ [*T. H. 2009*]

Let $C = \cos\alpha + \cos(\alpha+\beta) + \cos(\alpha+2\beta) + \cdots\cdots$

and $S = \sin\alpha + \sin(\alpha+\beta) + \sin(\alpha+2\beta) + \cdots\cdots$

Therefore $C + iS = (\cos\alpha + i\sin\alpha) + \{\cos(\alpha+\beta) + i\sin(\alpha+\beta)\}$

$$+ \{\cos(\alpha+2\beta) + i\sin(\alpha+2\beta)\} + \cdots\cdots \text{ to } n \text{ terms}$$

$$= e^{i\alpha} + e^{i(\alpha+\beta)} + e^{i(\alpha+2\beta)} + \cdots\cdots \text{ to } n \text{ terms} .$$

Hence $C + iS = e^{i\alpha} \cdot \dfrac{(e^{i\beta})^n - 1}{e^{i\beta} - 1} = e^{i\alpha} \cdot \dfrac{e^{in\beta} - 1}{e^{i\beta} - 1}$

$$= e^{i\alpha} \cdot \frac{\frac{1}{2i}\left(e^{\frac{in\beta}{2}} - e^{\frac{-in\beta}{2}}\right)e^{\frac{in\beta}{2}}}{\frac{1}{2i}\left(e^{\frac{i\beta}{2}} - e^{\frac{-i\beta}{2}}\right)e^{\frac{i\beta}{2}}} = \frac{\sin\frac{n\beta}{2}}{\sin\frac{\beta}{2}} \cdot e^{i\left(\alpha + \frac{n\beta}{2} - \frac{\beta}{2}\right)}$$

$$= \frac{\sin\frac{1}{2}n\beta}{\sin\frac{1}{2}\beta}\left\{\cos\left(\alpha + \frac{n-1}{2}\beta\right) + i\sin\left(\alpha + \frac{n-1}{2}\beta\right)\right\}.$$

Since α and β are real, equating the real and the imaginary parts from both sides, we get

$$C = \frac{\sin\frac{1}{2}n\beta}{\sin\frac{1}{2}\beta}\cos\left(\alpha + \frac{n-1}{2}\beta\right) \text{ and } S = \frac{\sin\frac{1}{2}n\beta}{\sin\frac{1}{2}\beta}\sin\left(\alpha + \frac{n-1}{2}\beta\right).$$

This is known as $(C + iS)$ *method of summation.*

Second method :

$\cos\alpha + \cos(\alpha + \beta) + \cos(\alpha + 2\beta) + \ldots\ldots + \cos\{\alpha + (n-1)\beta\}$

$$= \frac{1}{2\sin\frac{1}{2}\beta}\left[2\cos\alpha\sin\frac{\beta}{2} + 2\cos(\alpha+\beta)\sin\frac{\beta}{2} + \ldots\ldots\right.$$

$$\left. \ldots\ldots + 2\cos\{\alpha + (n-1)\beta\ \sin\frac{\beta}{2}\right]$$

$$= \frac{1}{2\sin\frac{1}{2}\beta}\left[\sin\left(\alpha + \tfrac{1}{2}\beta\right) - \sin\left(\alpha - \tfrac{1}{2}\beta\right)\right.$$

$$+ \sin\left(\alpha + \tfrac{3}{2}\beta\right) - \sin\left(\alpha + \tfrac{1}{2}\beta\right) + \ldots\ldots$$

$$\left. \ldots\ldots + \sin\{\alpha + (n - \tfrac{1}{2})\beta\} - \sin\{(\alpha + (n - \tfrac{3}{2})\beta\}\right]$$

$$= \frac{1}{2\sin\frac{1}{2}\beta}\left[\sin\left\{\alpha + \left(n - \frac{1}{2}\right)\beta\right\} - \sin\left(\alpha - \frac{\beta}{2}\right)\right]$$

$$= \frac{1}{2\sin\frac{1}{2}\beta} \cdot 2\cos\left(\alpha + \frac{n-1}{2}\beta\right)\sin\frac{n\beta}{2}$$

$$= \frac{\sin\frac{1}{2}n\beta}{\sin\frac{1}{2}\beta}\cos\left(\alpha + \frac{n-1}{2}\beta\right).$$

Similarly, the second result may also be obtained .

Note. The sum of the sines and the sum of the cosines of n angles in A.P. are each equal to zero, when the common difference of the angles is an even multiple of $\dfrac{\pi}{n}$.

Examples I(C)

1. (*a*) From the definitions of sine and cosine of complex numbers, show that

(*i*) $\sin x = 2 \sin \frac{1}{2}x \cos \frac{1}{2}x$.

(*ii*) $\cos 2x = 2\cos^2 x - 1 = 1 - 2\sin^2 x = \cos^2 x - \sin^2 x$.

(*iii*) $\sin 3x = 3\sin x - 4\sin^3 x$.

(*iv*) $\cos 3x = 4\cos^3 x - 3\cos x$.

(*v*) $\sin x + \sin y = 2\sin \frac{1}{2}(x+y)\cos \frac{1}{2}(x-y)$.

(*vi*) $\cos x + \cos y = 2\cos \frac{1}{2}(x+y)\cos \frac{1}{2}(x-y)$.

(*vii*) $\tan(z_1 + z_2) = \dfrac{\tan z_1 + \tan z_2}{1 - \tan z_1 \tan z_2}$.

(*viii*) $\dfrac{1 + \cos\theta + i\sin\theta}{1 + \cos\theta - i\sin\theta} = \cos\theta + i\sin\theta$.

(*b*) From the definitions of hyperbolic functions of complex numbers, show that

(*i*) $\sinh 3x = 4\sinh^3 x + 3\sinh x$.

(*ii*) $\cosh 3x = 4\cosh^3 x - 3\cosh x$.

(*iii*) $\tanh 3x = \dfrac{3\tanh x + \tanh^3 x}{1 + 3\tanh^2 x}$.

(*iv*) $(\cosh x \pm \sinh x)^n = \cosh nx \pm \sinh nx$, n being any integer.

(*v*) $\sinh^{-1} x = \cosh^{-1}\sqrt{1+x^2} = \tanh^{-1}\dfrac{x}{\sqrt{1+x^2}}$.

2. Show that

(*i*) $\mathrm{Log}(-i) = (4n+3)\frac{1}{2}\pi i$. [*B. H. 2003*]

(*ii*) $\mathrm{Log}(-1) = (2n+1)\pi i$. [*N. B. H. 1988*]

(*iii*) $\mathrm{Log}\sqrt{i} = \frac{1}{4}(8n+1)\pi i$.

(*iv*) $\mathrm{Log}_e(1+i) = \frac{1}{2}\log 2 + (2n + \frac{1}{4})\pi i$.

(*v*) $(i)^{-i} = e^{(2n+\frac{1}{2})\pi}$.

(*vi*) $(-i)^{-i} = e^{(4n-1)\frac{\pi}{2}}$.

(*vii*) $(-i)^{i} = e^{(2n+\frac{1}{2})\pi}$.

(*viii*) $\cos(\log i^{i}) = 0$.

(*ix*) $\sin(\log i^{i}) = -1$. [*C. H. 2009*]

(x) $i\log\frac{x-i}{x+i} = \pi - 2\tan^{-1}x$, if $x>0$

$= -\pi - 2\tan^{-1}x$, if $x\le 0$. [C. H. 2009]

(xi) $\cos\left(i\log\frac{a-ib}{a+ib}\right)=\frac{a^2-b^2}{a^2+b^2}$.

(xii) $\tan\left(i\log\frac{a-ib}{a+ib}\right)=\frac{2ab}{a^2-b^2}$. [K. H. 1979]

(xiii) $x^i = e^{-2n\pi}\{\cos(\log x)+i\sin(\log x)\}$.

(xiv) $\text{Log}_i\, i=\frac{4m+1}{4n+1}$, where m and n are integers.

(xv) $\text{Log}_e\frac{(a-b)+i(a+b)}{(a+b)+i(a-b)}=i\left(2n\pi+\tan^{-1}\frac{2ab}{a^2-b^2}\right)$.

(xvi) $\log\frac{a+x+iy}{a-x+iy}=\frac{1}{2}\log\frac{(a+x)^2+y^2}{(a-x)^2+y^2}$

$+i\left(\tan^{-1}\frac{y}{a+x}-\tan^{-1}\frac{y}{a-x}\right)$.

(xvii) $(\sin\theta+i\cos\theta)^i = e^{2n\pi+\theta-\frac{\pi}{2}}$.

(xviii) $\text{Sin}^{-1}ix = n\pi+(-1)^n i\log(x+\sqrt{1+x^2})$.

(xix) $i^\theta = \cos(2n+\frac{1}{2})\pi\theta + i\sin(2n+\frac{1}{2})\pi\theta$.

(xx) $\tan^{-1}(\cos\theta+i\sin\theta)=\frac{1}{4}\pi+\frac{1}{2}i\log\tan(\frac{1}{4}\pi+\frac{1}{2}\theta)$.

3. (a) Express the following in the form $(A+iB)$:

(i) $\cos(\theta+i\phi)$. (ii) $\tan(\theta+i\phi)$. [C. H. 1962]

(iii) $\sec(x+iy)$. (iv) $\text{cosec}(x+iy)$.

(v) $\cot(\alpha+i\beta)$. (vi) $\tan^{-1}(x+iy)$. [C. H. 1990]

(vii) $\text{Cos}^{-1}i$. (viii) $\text{Sin}^{-1}3$.

(ix) $e^{\alpha+i\beta}$. (x) $\text{Log}\{\log(\cos\theta+i\sin\theta)\}$.

(xi) $(1+i)^{1+i}$. (xii) i^{i^i}.

(xiii) $\log_e\{(\sqrt{3}+1)+i(\sqrt{3}-1)\}$.

(xiv) $\text{Log}\sin(x+iy)$. (xv) $\text{Log Log}(x+iy)$.

(xvi) $\cosh(x+iy)$.

(*b*) Separate $\tanh(x+iy)$ into real and imaginary parts.

(*c*) Find the real and imaginary parts of e^z, where $z=x+iy$, $0\le y<\pi$. Also find $|e^z|$ and $\arg e^z$. [*V. H. 1991*]

Show that $|e^z|\le e^{|z|}$. [*B. H. 1998*]

4. (*a*) If $\tan\log(x+iy)=a+ib$, where $a^2+b^2\neq 1$, then prove that $\tan\log(x^2+y^2)=\dfrac{2a}{1-a^2-b^2}$. [*N. B. H. 2006*]

(*b*) If $\log\sin(\theta+i\phi)=\alpha+i\beta$, then prove that

$$2\cos 2\theta = e^{2\phi}+e^{-2\phi}-4e^{2\alpha}$$

and $\cos(\theta-\beta)=e^{2\phi}\cos(\theta+\beta)$. [*C. H. 1970, 2009*]

5. (*a*) If $\alpha+i\beta=\cos(\theta+i\phi)$, then prove that

$$\frac{\alpha^2}{\cos^2\theta}-\frac{\beta^2}{\sin^2\theta}=1 \text{ and } \frac{\alpha^2}{\cosh^2\phi}+\frac{\beta^2}{\sinh^2\phi}=1.$$

In other words, show that $\cos^2\theta$ and $\cosh^2\phi$ are the roots of the equation $x^2-x(1+\alpha^2+\beta^2)+\alpha^2=0$.

(*b*) If $x+iy=c\cos(u+iv)$, then prove that

$u=$ constant represents a family of confocal hyperbolas and $v=$ constant represents a family of confocal ellipses. [*C. H. 1963*]

(*c*) If $x+iy=c\cosh(u+iv)$, then show that $u=$ constant represents a family of confocal hyperbolas. [*K. H. 2006*]

6. (*a*) If $u+iv=\cot(x+iy)$, then show that

$$u^2+v^2-2u\cot 2x=1$$

and $$u^2+v^2+2v\coth 2y+1=0.$$

(*b*) If $u+iv=\operatorname{cosec}(x+iy)$, then show that

$$(u^2+v^2)^2=\frac{u^2}{\sin^2 x}-\frac{v^2}{\cos^2 x}=\frac{u^2}{\cosh^2 y}+\frac{v^2}{\sinh^2 y}.$$

7. If $\tan^{-1}(u+iv)=\sin^{-1}(a+ib)$, then show that

$$u^2+v^2=\frac{a^2+b^2}{\sqrt{(a^2+b^2)^2-2a^2+2b^2+1}}.$$

8. If $x+iy=a\cos(u+iv)+ib\sin(u+iv)$, then show that

$$\frac{x^2}{\cos^2 u}-\frac{y^2}{\sin^2 u}=a^2-b^2.$$

9. Show that the values of i^i are all real and they can be arranged so that they form a G.P. [*C. H. 1984*]

10. (*a*) If $i^{\alpha+i\beta} = \alpha + i\beta$, then prove that $\alpha^2 + \beta^2 = e^{-(4n+1)\pi\beta}$. [*N. B. H. 2011*]

(*b*) If a, b, p be real and $|a+ib| = 1$, then show that $(a+ib)^{ip}$ is purely real.

11. (*a*) If $x = \log\tan(\frac{1}{4}\pi + \frac{1}{2}y)$, then prove that ($x, y$ being real) $y = -i\,\mathrm{Log}\tan(\frac{1}{4}\pi + \frac{1}{2}ix)$. [*V. H. 1988, C. H. 1989, K. H. 2005*]

[Here $e^x = \dfrac{1+\tan\frac{1}{2}y}{1-\tan\frac{1}{2}y}$, giving $\tan\dfrac{y}{2} = \dfrac{e^x-1}{e^x+1}$.

Hence $\dfrac{e^{\frac{iy}{2}} - e^{-\frac{iy}{2}}}{i(e^{\frac{iy}{2}} + e^{-\frac{iy}{2}})} = \dfrac{e^{\frac{x}{2}} - e^{-\frac{x}{2}}}{e^{\frac{x}{2}} + e^{-\frac{x}{2}}} = -i\tan\dfrac{ix}{2}$.

Therefore $e^{iy} = \dfrac{1+\tan\frac{1}{2}ix}{1-\tan\frac{1}{2}ix} = \tan\left(\dfrac{\pi}{4} + \dfrac{ix}{2}\right)$.]

(*b*) If $y = \log\tan(\frac{1}{4}\pi + \frac{1}{2}x) = x + c_3x^3 + c_5x^5 + \cdots\cdots$, then prove that $x = y - c_3y^3 + c_5y^5 - \cdots\cdots$. [*V. H. 2010*]

12. Find the principal values of

(*i*) $\mathrm{Log}(1+i)$. (*ii*) $\mathrm{Log}(-\frac{1}{2} - \frac{1}{2}i\sqrt{3})$. [*C. H. 1968*]

13. Show that the ratio of the principal values of

(*i*) $(1+i)^{1-i}$ and $(1-i)^{1+i}$ is $\sin(\log 2) + i\cos(\log 2)$. [*C. H. 1977, 2005; V. H. 1989*]

(*ii*) $(x+iy)^{a+ib}$ and $(x-iy)^{a-ib}$ is $\cos 2(a\theta + b\log r) + i\sin 2(a\theta + b\log r)$,

where $r = \sqrt{x^2+y^2}$ and $\theta = \tan^{-1}\dfrac{y}{x}$.

14. (*a*) If a, b, z be complex numbers such that $ab \neq 0$, then prove that $(ab)^z = a^z b^z$ but the principal value of $(ab)^z$ is not equal to the product of the principal values of a^z and b^z. [*C. H. 1996*]

(*b*) Show that $\mathrm{Log}\,i^2 \neq 2\,\mathrm{Log}\,i$, but $\log i^2 = 2\log i$.

15. (*a*) Solve : (*i*) $\sin z = 0$. (*ii*) $\cos z = 0$.
(*iii*) $e^{2z+1} = i$. (*iv*) $e^z = 1 + i\sqrt{3}$.

(*b*) Find z, such that

(*i*) $\sin z = 2$. (*ii*) $\sinh z = 1$. (*iii*) $\sinh z = 2i$.
(*iv*) $\cosh z = -2$. (*v*) $\tan z = 2 + i$.

(*c*) Show that the solution of the equation

(*i*) $\cos x = 2$ is given by $x = 2n\pi \pm i\log(2+\sqrt{3})$, n being an integer. [*C. H. 1977; K. H. 2005*]

(*ii*) $\cos z = -2$ is given by

$z = (2n+1)\pi \pm i \log(2-\sqrt{3})$. [*C. H. 1986*]

(*iii*) $\cos x = c$, c being any real number greater than 1, is given by $x = 2n\pi \pm i \log(c+\sqrt{c^2-1})$.

(*iv*) $\sin x = c$, where c is any real number greater than 1, is given by $x = n\pi + (-1)^n \left\{ \frac{1}{2}\pi - i \log\left(c+\sqrt{c^2-1} \right) \right\}$.

16. (*a*) Solve : $\cos(x+iy) = \frac{5}{4}$.

(*b*) Prove that the general values of $\tan^{-1}(1+i)$ are

$$(n+\tfrac{1}{2})\pi + \tfrac{1}{2}\tan^{-1}(-2) + i \cdot \tfrac{1}{4}\log 5 .$$

(*c*) Show that the general solution of

$\tan^{-1} e^{ix} - \tan^{-1} e^{-ix} = \tan^{-1} i$ is $x = n\pi + \frac{1}{2}(-1)^n \pi$.

17. (*a*) Show that the general value of $(1+i\tan\alpha)^{-i}$ is

$e^{\alpha+2n\pi} \{\cos(\log\cos\alpha) + i\sin(\log\cos\alpha)\}$.

(*b*) Find the general values and the principal value of

$i^{\log(1+i)}$. [*C. H. 1988*]

(*c*) If $(1+i\tan\alpha)^{1+i\tan\beta}$ can have real values, then show that one of them is $(\sec\alpha)^{\sec^2\beta}$.

18. If z be complex, then show that

$\sin\overline{z} = \overline{\sin z}$, $\cos\overline{z} = \overline{\cos z}$ and $\tan\overline{z} = \overline{\tan z}$.

19. (*a*) If $z = x+iy$, then prove that

$|\sinh y| \le |f(z)| \le \cosh y$, where $f(z) = \sin z$ or $\cos z$.

(*b*) If $x > 0$, then show that

$\cosh x > \sinh x > x > \tanh x$.

(*c*) For any complex number z, prove that

$|\cos z| \le \cosh|z|$ and $|\sin z| \le \sinh|z|$.

20. If α and β be real and

(*i*) $|\sin(\alpha+i\beta)| = 1$, then prove that $\cosh 2\beta - \cos 2\alpha = 2$.

(*ii*) $|\cos(\alpha+i\beta)| = 1$, then prove that $\sin^2\alpha = \sinh^2\beta$.

[*C. H. 1963, 1980, 1988*]

21. If $\tan(\theta+i\phi) = \sin(\alpha+i\beta)$, then show that

$\coth\beta \sinh 2\phi = \cot\alpha \sin 2\theta$.

22. If $i^{i^{i^{\text{to}\infty}}} = A + iB$, then prove that $\tan \frac{1}{2}\pi A = \frac{B}{A}$ and $A^2 + B^2 = e^{-\pi B}$, by considering the principal values only.

23. (*a*) If $\tan(\theta + i\phi) = \tan\beta + i\sec\beta$, $0 < \beta < \pi$, then show that $e^{2\phi} = \cot\frac{1}{2}\beta$ and $2\theta = \frac{1}{2}\pi + \beta$. [*C. H. 1980*]

[Here $\frac{\sin(\theta + i\phi)}{\cos(\theta + i\phi)} = \frac{\sin\beta + i}{\cos\beta}$, that is, $\frac{\cos(\theta + i\phi)}{i\sin(\theta + i\phi)} = \frac{\cos\beta}{i\sin\beta - 1}$.

Apply componendo and dividendo.]

(*b*) If $\sin(\theta + i\phi) = \tan\beta + i\sec\beta$, then show that

$$\cos 2\theta \cosh 2\phi = 3.$$

(*c*) If $x + iy = \tan^{-1}(\tan\phi + i\sec\phi)$, $0 < \phi < \frac{1}{2}\pi$, then prove that

$$x = n\pi + \tfrac{1}{4}\pi + \tfrac{1}{2}\phi,\ y = \tfrac{1}{4}\log\frac{1 + \cos\phi}{1 - \cos\phi}.$$

(*d*) If $\cosh(x + iy) = \cot(u + iv)$, then prove that

$$\frac{\sinh 2v}{\sin 2u} = -\tanh x \tan y.$$ [*C. H. 1996*]

24. (*a*) If $\cosh^{-1}(x + iy) - \cosh^{-1}(x - iy) = \cosh^{-1} c$, then show that $2(1 - c)x^2 - 2(1 + c)y^2 = 1 - c^2$. [*V. H. 2003*]

(*b*) If $\sinh^{-1}(x + iy) + \sinh^{-1}(x - iy) = \cosh^{-1} a$, where a is a constant greater than 1, then prove that (x, y) lies on an ellipse. [*C. H. 1994*]

If $a < 1$, then show that the curve will be a hyperbola.

25. Show that the points a^z lie on the equiangular spiral

$$r = \sigma^{\frac{1}{u}(u^2 + v^2)} e^{-\frac{v}{u}\theta}, \text{ where } z = u + iv \text{ and}$$

$$a = \sigma(\cos\psi + i\sin\psi),\ -\pi < \psi \le \pi.$$ [*C. H. 1980*]

26. Considering the principal values of logarithms of both sides of the equality $(a + ib)^p = m^{x+iy}$, where $a > b > 0$, $p > 0$, $m > 1$, $x > 0$, $y > 0$, show that

$$\tan\left\{\frac{y}{x}\log\left(a^2 + b^2\right)\right\} = \frac{2ab}{a^2 - b^2}.$$ [*C. H. 1982*]

27. (*a*) Given that $\sin x = u\sin(x + \alpha)$, expand x in powers of u $(-1 < u < 1)$.

(*b*) If $\tan x = n\tan y$, then find a series for x.

28. Expand $\log(1-2x\cos\theta+x^2)$ in a series of cosines of multiples of θ.

29. Deduce from the Gregory's series

(*i*) $\frac{\pi}{8}=\frac{1}{1.3}+\frac{1}{5.7}+\frac{1}{9.11}+\cdots\cdots$ [*T. H. 2008*]

[Put $\theta=\frac{1}{4}\pi$ in Gregory's series and obtain

$\frac{1}{4}\pi=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots\cdots=(1-\frac{1}{3})+(\frac{1}{5}-\frac{1}{7})+\cdots\cdots$ and proceed.]

(*ii*) $\pi=2\sqrt{3}\left(1-\frac{1}{3.3}+\frac{1}{5.3^2}-\frac{1}{7.3^3}+\cdots\cdots\right)$.

(*iii*) $\frac{\pi}{4}=\left(\frac{2}{3}+\frac{1}{7}\right)-\frac{1}{3}\left(\frac{2}{3^3}+\frac{1}{7^3}\right)+\frac{1}{5}\left(\frac{2}{3^5}+\frac{1}{7^5}\right)-\cdots\cdots$ [*T. H. 2009*]

(*iv*) $\frac{1}{4}\pi=\cos\theta-\frac{1}{3}\cos3\theta+\frac{1}{5}\cos5\theta-\cdots\cdots$

and $\frac{1}{2}\log\tan(\frac{1}{4}\pi+\frac{1}{2}\theta)=\sin\theta-\frac{1}{3}\sin3\theta+\frac{1}{5}\sin5\theta-\cdots\cdots$

when $0<\theta<\frac{1}{2}\pi$.

(*v*) $\tan^{-1}\frac{1-\cos\theta}{1+\cos\theta}=\tan^2\frac{\theta}{2}-\frac{1}{3}\tan^6\frac{\theta}{2}+\frac{1}{5}\tan^{10}\frac{\theta}{2}-\cdots\cdots$,

if $-\frac{1}{2}\pi\le\theta\le\frac{1}{2}\pi$.

30. Find the sum to n terms of the series :

(*i*) $\sin\alpha+\sin3\alpha+\sin5\alpha+\cdots\cdots$ [*K. H. 1997*]

(*ii*) $\sin\alpha+\sin\left(\alpha+\frac{\pi}{n}\right)+\sin\left(\alpha+\frac{2\pi}{n}\right)+\cdots\cdots$

(*iii*) $\sin^2\alpha+\sin^2(\alpha+\beta)+\sin^2(\alpha+2\beta)+\cdots\cdots$

(*iv*) $\cos^3\alpha+\cos^3(\alpha+\beta)+\cos^3(\alpha+2\beta)+\cdots\cdots$

(*v*) $\cos^3x+\cos^32x+\cos^33x+\cdots\cdots+\cos^3nx$. [*V. H. 1989*]

31. For any real triangle ABC, prove that

$(\cos A+i\sin A)(\cos B+i\sin B)(\cos C+i\sin C)$

is real and find its simplest value.

32. If θ be real, resolve $P=e^{e^{i\theta}}$ into real and imaginary parts and then substantiate the following statements :

(*i*) that P cannot be purely imaginary

and (*ii*) that, if P be purely real, it must be equal to either e or e^{-1}.

In case (*ii*), note also the corresponding value of θ.

Answers

3. (*a*) (*i*) $\frac{1}{2}(e^{-\phi}+e^{\phi})\cos\theta + i\frac{1}{2}(e^{-\phi}-e^{\phi})\sin\theta$.

(*ii*) $\dfrac{\sin 2\theta}{\cosh 2\phi+\cos 2\theta} + i\dfrac{\sinh 2\phi}{\cosh 2\phi+\cos 2\theta}$.

(*iii*) $\dfrac{2\cos x\cosh y}{\cos 2x+\cosh 2y} + i\dfrac{2\sin x\sinh y}{\cos 2x+\cosh 2y}$.

(*iv*) $\dfrac{2\sin x\cosh y}{1-\cos 2x\cosh 2y} - i\dfrac{2\cos x\sinh y}{1-\cos 2x\cosh 2y}$.

(*v*) $\dfrac{\sin 2\alpha}{\cosh 2\beta-\cos 2\alpha} - i\dfrac{\sinh 2\beta}{\cosh 2\beta-\cos 2\alpha}$.

(*vi*) $\dfrac{1}{2}\tan^{-1}\dfrac{2x}{1-x^2-y^2} + i\dfrac{1}{2}\tanh^{-1}\dfrac{2y}{1+x^2+y^2}$.

(*vii*) $(2n\pi\pm\frac{1}{2}\pi)\mp i\log(\sqrt{2}+1)$.

(*viii*) $(2n\pi+\frac{1}{2}\pi)\pm i\log(2\sqrt{2}+3)$.

(*ix*) $e^{\alpha}\cos\beta + i\,e^{\alpha}\sin\beta$.

(*x*) $\log\theta + i(2n\pi+\frac{1}{2}\pi)$.

(*xi*) $e^{\frac{1}{2}\log 2-2n\pi-\frac{\pi}{4}}\cdot\cos(2n\pi+\frac{1}{4}\pi+\frac{1}{2}\log 2)$
$+ ie^{\frac{1}{2}\log 2-2n\pi-\frac{\pi}{4}}\cdot\sin(2n\pi+\frac{1}{4}\pi+\frac{1}{2}\log 2)$.

(*xii*) $\cos\theta + i\sin\theta$, where $\theta=\frac{1}{2}(4m+1)\pi e^{-(4n+1)\frac{\pi}{2}}$.

(*xiii*) $\frac{3}{2}\log_e 2+\frac{1}{12}\pi i$.

(*xiv*) $\frac{1}{2}\log\left\{\frac{1}{2}(\cosh 2y-\cos 2x)\right\} + i\{2n\pi+\tan^{-1}(\cot x\tanh y)\}$.

(*xv*) $\dfrac{1}{2}\log\left[\left\{\frac{1}{2}\log(x^2+y^2)\right\}^2+\left(2n\pi+\tan^{-1}\frac{y}{x}\right)^2\right]$
$+ i\left\{2m\pi+\tan^{-1}\dfrac{2n\pi+\tan^{-1}\frac{y}{x}}{\frac{1}{2}\log(x^2+y^2)}\right\}$.

(*xvi*) $\cosh x\cos y + i\sinh x\sin y$.

(*b*) $\dfrac{\sinh 2x+i\sin 2y}{\cosh 2x+\cos 2y}$.

(*c*) $e^x\cos y$, $e^x\sin y$; e^x, y.

12. (*i*) $\frac{1}{2}\log 2+\frac{1}{4}\pi i$.

(*ii*) $\frac{4}{3}\pi i$.

15. (*a*) (*i*) $n\pi$. (*ii*) $n\pi+\frac{1}{2}\pi$. (*iii*) $-\frac{1}{2}+\frac{1}{4}(4n+1)\pi i$.

(*iv*) $\log 2+(2n+\frac{1}{3})\pi i$.

(*b*) (*i*) $n\pi+(-1)^n\left\{\frac{1}{2}\pi-i\log(2+\sqrt{3})\right\}$.

(*ii*) $n\pi i+(-1)^n\log(1+\sqrt{2})$.

(*iii*) $\log(2\pm\sqrt{3})+(2n+\frac{1}{2})\pi i$.

(*iv*) $\log(2\pm\sqrt{3})+(2n+1)\pi i$.

(*v*) $\left(n+\frac{3}{8}\right)\pi+\frac{1}{4}i\log 2$.

16. (*a*) $x=2n\pi$, $y=\pm\log 2$.

17. (*b*) $e^{-(4n+1)\frac{\pi^2}{8}}\left\{\cos\frac{1}{4}(4n+1)\pi\log 2+i\sin\frac{1}{4}(4n+1)\pi\log 2\right\}$;

$e^{-\frac{\pi^2}{8}}\left\{\cos\left(\frac{1}{4}\pi\log 2\right)+i\sin\left(\frac{1}{4}\pi\log 2\right)\right\}$.

27. (*a*) $u\sin\alpha+\frac{1}{2}u^2\sin 2\alpha+\frac{1}{3}u^3\sin 3\alpha+\cdots\cdots$.

(*b*) $x=y-k\sin 2y+\frac{1}{2}k^2\sin 4y-\frac{1}{3}k^3\sin 6y+\cdots\cdots$, where $k=\dfrac{1-n}{1+n}$.

28. $-2\left(x\cos\theta+\frac{1}{2}x^2\cos 2\theta+\frac{1}{3}x^3\cos 3\theta+\cdots\cdots\right)$.

30. (*i*) $\dfrac{\sin^2 n\alpha}{\sin\alpha}$. (*ii*) $\dfrac{\cos\left(\alpha-\dfrac{\pi}{2n}\right)}{\sin\dfrac{\pi}{2n}}$.

(*iii*) $\dfrac{n}{2}-\dfrac{1}{2}\dfrac{\sin n\beta\cos\{2\alpha+(n-1)\beta\}}{\sin\beta}$.

(*iv*) $\frac{1}{4}\sin\frac{3}{2}n\beta\cdot\cos\{3\alpha+\frac{3}{2}(n-1)\beta\}\operatorname{cosec}\frac{3}{2}\beta$

$+\frac{3}{4}\sin\frac{1}{2}n\beta\cdot\cos\{\alpha+\frac{1}{2}(n-1)\beta\}\operatorname{cosec}\frac{1}{2}\beta$.

(*v*) $\dfrac{1}{4}\sin\dfrac{3nx}{2}\cos\dfrac{3(n+1)x}{2}\operatorname{cosec}\dfrac{3x}{2}+\dfrac{3}{4}\sin\dfrac{nx}{2}\cos\dfrac{(n+1)x}{2}\operatorname{cosec}\dfrac{x}{2}$.

31. -1. 32. $e^{\cos\theta}\cos(\sin\theta)+i\cdot e^{\cos\theta}\sin(\sin\theta)$; 0 or π.

2 THEORY OF EQUATIONS (1)

2.1. Polynomials.

An algebraical symbol x is called a continuous *real variable*, if it passes once through all real values between any two numbers a and b. A mathematical expression involving the variable x is called a *function* of x, if its value depends upon that of x. This statement is indicated by the symbols $f(x), F(x), \phi(x), \psi(x)$, etc. There are different classes of functions, such as, algebraical functions : $3x^2 - 7x + 2$; trigonometric functions: $\sin x$, $\sec x$; transcendental functions : e^x, $\log x$; and so on. An algebraical function in which the variable is free from fractional indices is called *rational*. It is called *integral*, if the variable does not occur in the denominator of a function.

A rational integral function of the form

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots\cdots + a_n,$$

in which $a_0, a_1, a_2, \ldots\ldots, a_n$ are independent of x, is called a *polynomial* in x. The coefficients $a_0, a_1, a_2, \ldots\ldots, a_n$ are called *constants*. The *degree* of the polynomial is that of its highest degree term. Thus a constant may be regarded as a polynomial of degree zero. Polynomials of the first, second, third, fourth,..... degree are called *linear, quadratic, cubic, quartic* (*biquadratic*),.....functions respectively.

A *complete* polynomial contains all the lower degree terms beginning from the highest; otherwise it is an incomplete polynomial.

A polynomial in x is a continuous function of x.

A polynomial in two variables x and y is an expression involving terms of the form $ax^m y^n$, where a is independent of x and y, and m and n are positive integers. A polynomial in any number of variables is similarly defined. The largest value of the sum of the indices of the variables in each term determines the *degree* of such polynomials. If this sum be constant for all the terms, then the polynomial is said to be homogeneous. For instance,

$$3x^4 + 5x^3 y - 2x^2 y^2 + 9xy^3 + y^4$$

is a homogeneous polynomial in x, y of degree 4.

A polynomial of only one term is called a *monomial*; a polynomial of two terms is called a *binomial*; a polynomial of three terms is called a *trinomial*.

Thus $3x$ is a monomial, $(2x+3)$ is a binomial and $(3x^2+2x-3)$ is a trinomial.

Each of the sum, difference and product of two polynomials is itself a polynomial. If $f(x), \phi(x)$ and $\psi(x)$ be polynomials in x and $f(x)=\phi(x)\,\psi(x)$, then $\phi(x)$ and $\psi(x)$ are called the *factors* of $f(x)$.

The *graphical representation* of a polynomial $f(x)$ is equivalent to tracing the plane curve $y=f(x)$ as is done in analytical geometry of two dimensions.

2.2. Division of polynomials.

If $f(x)$ be of higher degree than $\phi(x)$ (or of the same degree), then to divide $f(x)$ by $\phi(x)$ is to find an identity of the form

$$f(x)=\phi(x)\cdot Q+R,$$

where Q and R are polynomials in x and R is of lower degree than $\phi(x)$. Q is called the *quotient* and R, the *remainder*. Such division of two polynomials is always possible and is known as *division algorithm*. In this process, Q and R are unique.

If $R=0$, then $f(x)$ is completely divisible by $\phi(x)$ and $\phi(x)$ is a factor of $f(x)$.

2.3. Synthetic division.

This is a process to divide any polynomial $f(x)$ in x by a binomial of the form $(x-h)$. Let

$$f(x)\equiv a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots\cdots+a_n,\ a_0\neq 0.$$

By algorithms of division, we have

$$f(x)\equiv(x-h)\cdot Q(x)+R, \qquad \ldots \quad (1)$$

where R, the remainder, is obviously a constant.

Let $Q(x)=b_0x^{n-1}+b_1x^{n-2}+b_2x^{n-3}+\cdots\cdots+b_{n-1}$.

The coefficients of like powers of x on both sides of the identity (1) must be equal. On actual multiplication, the right hand side of (1) becomes

$$b_0x^n+(b_1-hb_0)x^{n-1}+(b_2-hb_1)x^{n-2}+\cdots\cdots+(b_{n-1}-hb_{n-2})x+R-hb_{n-1}.$$

Equating the coefficients of like powers of x, we have

$$a_0=b_0,\ a_1=b_1-hb_0,\ a_2=b_2-hb_1,\ldots\ldots,a_n=R-hb_{n-1}.$$

Hence $b_0=a_0,\ b_1=hb_0+a_1,\ b_2=hb_1+a_2,\ldots\ldots,R=hb_{n-1}+a_n.$

Thus we have an easy process of calculating the coefficients of the quotient polynomial and the remainder as follows :

$$\begin{array}{cccccccc} a_0 & a_1 & a_2 & a_3 & \ldots\ldots & a_{n-1} & a_n \\ & b_0h & b_1h & b_2h & \ldots\ldots & b_{n-2}h & b_{n-1}h \\ \hline b_0 & b_1 & b_2 & b_3 & \ldots\ldots & b_{n-1} & R \end{array}$$

The arrangement is as follows :

The first row contains the coefficients of the dividend polynomial arranged in descending powers of x, the missing terms of an incomplete polynomial being supplied with zero coefficients. The first place in the second row is kept blank.

We put $b_0 (= a_0)$ in the first place on the third row just below a_0. b_0 is multiplied by h and the product is placed in the second row just below a_1. b_1 in the third row is the sum of a_1 and b_0h and this becomes the coefficient of the second term of the quotient polynomial. This process is continued to get the coefficients $b_2, b_3, \ldots\ldots, b_{n-1}$ of the quotient polynomial.

Multiplying b_{n-1} by h, we put hb_{n-1} in the second row below a_n and we get the remainder $R = a_n + b_{n-1}h$.

Note. To divide a polynomial $f(x)$ by $(ax-b)$, we are first to find the quotient Q and the remainder R in the division of $f(x)$ by $\left(x-\frac{b}{a}\right)$.

Then $\frac{Q}{a}$ and R are respectively the quotient and the remainder in the division of $f(x)$ by $(ax-b)$; for, $f(x) = \left(x-\frac{b}{a}\right)Q + R = (ax-b)\frac{Q}{a} + R$.

2.4. Remainder theorem.

If a polynomial $f(x)$ be divided by a binomial $(x-h)$, then the remainder is $f(h)$.

Let Q be the quotient and R be the remainder, independent of x, when $f(x)$ is divided by $(x-h)$.

Then $f(x) = (x-h)Q + R$.

Putting $x = h$, we have $f(h) = 0.Q + R = R$.

Cor. If $f(x)$ vanishes for $x = h$, then $(x-h)$ is a factor of $f(x)$.

Since $f(h) = 0$, we have $R = 0$.

Hence $f(x) = (x-h)Q$, that is, $(x-h)$ is a factor of $f(x)$.

Note. $f(x)$ is completely divisible by $(x-h)$, if and only if $f(h)=0$. The value or values of x for which the polynomial $f(x)$ vanishes are called the *zeros* of the polynomial.

2.5. Application of Remainder theorem.

(*a*) *If* $f(x)$ *be a polynomial which vanishes when* x *has the values* $p_1, p_2, \ldots\ldots, p_n$, *no two of which are equal, then the product* $(x-p_1)(x-p_2)\ldots\ldots(x-p_n)$ *is a factor of* $f(x)$.

Since $f(p_1)=0$, by Remainder theorem,

$$f(x)=(x-p_1)f_1(x), \qquad \ldots \quad (1)$$

where $f_1(x)$ is a polynomial.

Putting $x=p_2$ in (1), we get

$$f(p_2)=(p_2-p_1)f_1(p_2).$$

Now $(p_2-p_1)\neq 0$ and $f(p_2)=0$.

Consequently, $f_1(p_2)=0$.

Therefore $(x-p_2)$ is a factor of $f_1(x)$.

Hence $f_1(x)=(x-p_2)f_2(x)$

and $f(x)=(x-p_1)(x-p_2)f_2(x)$, where $f_2(x)$ is a polynomial.

Proceeding in this way, it can be shown that

$(x-p_1)(x-p_2)\ldots\ldots(x-p_n)$ is a factor of $f(x)$.

(*b*) *A polynomial* $f(x)$ *of n-th degree cannot vanish for more than n values of x unless all its coefficients are zero.*

If $f(x)=0$ for more than n values $p_1, p_2, \ldots\ldots, p_m, (m>n)$, of x, then the product $(x-p_1)(x-p_2)\ldots\ldots(x-p_m)$ of more than n linear expressions would be a factor of the polynomial. Thus a polynomial of n-th degree will have a factor whose degree is higher than n, which is impossible.

Hence the theorem follows.

Cor. In case a polynomial of degree n vanishes for more than n values of x, then all its coefficients are zero and the polynomial is said to vanish identically.

(*c*) *If for more than n values of x,*

$$a_0x^n+a_1x^{n-1}+\ldots\ldots+a_{n-1}x+a_n=b_0x^n+b_1x^{n-1}+\ldots\ldots+b_{n-1}x+b_n,$$

then $a_0=b_0, a_1=b_1, \ldots\ldots, a_{n-1}=b_{n-1}, a_n=b_n$,

that is to say, the polynomials are identically equal.

By the given condition, the polynomial

$$(a_0-b_0)x^n+(a_1-b_1)x^{n-1}+\cdots\cdots+(a_{n-1}-b_{n-1})x+(a_n-b_n)$$

vanishes for more than n values of x. Hence its coefficients are zero.

Thus $a_0=b_0,\ a_1=b_1,\ldots\ldots,a_{n-1}=b_{n-1},a_n=b_n$.

(d) To express a given function $f(x)$ as a function of $(x-h)$.

Let $f(x)\equiv a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots\cdots+a_{n-1}x+a_n$. ... (1)

Let us suppose that, this can be expressed as

$$f(x)=b_0(x-h)^n+b_1(x-h)^{n-1}+\cdots\cdots+b_{n-1}(x-h)+b_n \quad \ldots (2)$$

$$=(x-h)\left\{b_0(x-h)^{n-1}+b_1(x-h)^{n-2}+\cdots\cdots+b_{n-1}\right\}+b_n$$

$$=(x-h)Q(x-h)+b_n \text{ (say)},$$

that is to say, $Q(x-h)$ is the quotient polynomial and b_n is the remainder when $f(x)$ is divided by $(x-h)$.

Thus, if the polynomial $f(x)$ be divided by $(x-h)$, then the remainder is b_n, the last coefficient of (2).

Again, if the quotient polynomial $Q(x-h)$ be divided by $(x-h)$, the remainder after division is b_{n-1}, which is the coefficient of $(x-h)$ in (2).

Proceeding in this way, we obtain, after each successive division, the coefficients $b_n, b_{n-1}, b_{n-2},\ldots\ldots,b_1$, the coefficient b_0 being equal to a_0.

The synthetic division method is applied for successive division; because at each stage of operation we get the quotient polynomial and the remainder in the same row.

Cor. To find $f(x+h)$ in powers of x, we express $f(x)$ as a polynomial in $(x-h)$ and then change x to $(x+h)$.

Note. If $f(x)$ be a polynomial of degree n in x, then *Taylor's finite expansion* of $f(x+h)$ in powers of h is

$$f(x+h)=f(x)+hf'(x)+\frac{h^2}{2!}f''(x)+\frac{h^3}{3!}f'''(x)+\cdots\cdots+\frac{h^n}{n!}f^n(x),$$

where $f'(x), f''(x),\ldots\ldots,f^n(x)$ denote the respective first, second,....., n-th derivatives of $f(x)$ with respect to x.

Using this also, we can find $f(x+h)$.

$f'(x), f''(x), f'''(x),\ldots\ldots$ are also called the respective first, second, third,..... *derived functions* of $f(x)$.

2.6. Two important theorems.

Theorem 1. *In the polynomial*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots\cdots + a_{n-1}x + a_n,\ a_0 \neq 0,$$

the leading term a_0x^n *numerically exceeds the sum of the remaining terms for*

$$|x| \geq \left(\frac{|a_k|}{|a_0|} + 1\right),$$

where a_k *is the greatest coefficient irrespective of signs.*

We have $|a_0x^n| \geq |a_1x^{n-1} + a_2x^{n-2} + \cdots\cdots + a_{n-1}x + a_n|$,

if $|a_0||x|^n \geq |a_1||x|^{n-1} + |a_2||x|^{n-2} + \cdots\cdots + |a_{n-1}||x| + |a_n|$,

that is, if $|a_0||x|^n \geq |a_k|\left(|x|^{n-1} + |x|^{n-2} + \cdots\cdots + |x| + 1\right)$,

$|a_k|$ being the greatest of $|a_1|, |a_2|, \ldots\ldots, |a_n|$

that is, if $|a_0||x|^n \geq |a_k|\dfrac{|x|^n - 1}{|x| - 1}$.

This holds if $\dfrac{|a_k|}{|a_0|(|x| - 1)} \leq 1$ and $|x| > 1$,

that is, if $|a_k| \leq |a_0|(|x| - 1)$,

that is, if $|x| - 1 \geq \dfrac{|a_k|}{|a_0|}$, that is, if $|x| \geq \dfrac{|a_k|}{|a_0|} + 1$.

Cor. For any value of $|x| \geq \dfrac{|a_k|}{|a_0|} + 1$, the sign of the polynomial will be the same as that of the term containing the highest power.

Theorem 2. *In the polynomial*

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots\cdots + a_{n-1}x + a_n, a_n \neq 0,$$

the constant term a_n *numerically exceeds the sum of the other terms for*

$$|x| \leq \frac{|a_n|}{|a_k| + |a_n|},$$

where a_k *is the greatest coefficient (except* a_n*) irrespective of signs.*

By putting $x = \dfrac{1}{y}$, the polynomial becomes

$$a_n + a_{n-1}\frac{1}{y} + a_{n-2}\frac{1}{y^2} + \cdots\cdots + a_1\frac{1}{y^{n-1}} + a_0\frac{1}{y^n}$$

$$= \frac{1}{y^n}\left(a_ny^n + a_{n-1}y^{n-1} + a_{n-2}y^{n-2} + \cdots\cdots + a_1y + a_0\right).$$

By the previous theorem, for $|y| \geq \frac{|a_k|}{|a_n|} + 1$,

$$|a_n y^n| > |a_{n-1}y^{n-1} + a_{n-2}y^{n-2} + \cdots\cdots + a_1 y + a_0|$$

that is, $|a_n| > |a_{n-1}\frac{1}{y} + a_{n-2}\frac{1}{y^2} + \cdots\cdots + a_1\frac{1}{y^{n-1}} + a_0\frac{1}{y^n}|$.

Replacing $\frac{1}{y}$ by x, we get

$$|a_n| > |a_{n-1}x + a_{n-2}x^2 + \cdots\cdots + a_1 x^{n-1} + a_0 x^n|,$$

if $\frac{1}{|x|} \geq \frac{|a_k| + |a_n|}{|a_n|}$, that is, if $|x| \leq \frac{|a_n|}{|a_k| + |a_n|}$.

Cor. For any value of $|x| \leq \frac{|a_n|}{|a_k| + |a_n|}$, the sign of the polynomial is the same as that of a_n.

2.7. Maximum and minimum values of a polynomial.

Any value of x, for which the polynomial $f(x)$ is a maximum or minimum, is a root of the derived equation $f'(x) = 0$. When $f''(x)$ is negative, then $f(x)$ is a maximum and when $f''(x)$ is positive, then $f(x)$ is a minimum. Thus $f(x)$ will be a maximum at $x = a$, if $f'(a) = 0$ and $f''(a) < 0$ and the maximum value is $f(a)$.

Similarly, $f(x)$ will be a minimum at $x = a$, if $f'(a) = 0$ and $f''(a) > 0$ and the minimum value is $f(a)$.

2.8. Illustrative Examples.

Ex.1. *If* $f(x) = x^3 - 3x^2 + 4x - 3$, *find* (*i*) $f(1)$ *and* (*ii*) $f(\sqrt{2})$.

(*i*) $f(1) = 1^3 - 3.1^2 + 4.1 - 3 = 1 - 3 + 4 - 3 = -1$.

(*ii*) $f(\sqrt{2}) = 2^{3/2} - 3.2 + 4.2^{1/2} - 3 = \sqrt{2}(2+4) - 9 = 6\sqrt{2} - 9$.

Ex. 2. *Find the remainder when* $(x^4 + 2x^3 - 13x^2 - 14x + 24)$ *is divided by* $(x+1)$. *Also show that the same expression is exactly divisible by* $(x-1)$.

Let $f(x) = x^4 + 2x^3 - 13x^2 - 14x + 24$. When $f(x)$ is divided by $(x+1)$ and $(x-1)$, the remainders are $f(-1)$ and $f(1)$ respectively.

Now $f(-1) = 1 - 2 - 13 + 14 + 24 = 24$

and $f(1) = 1 + 2 - 13 - 14 + 24 = 0$.

Thus the given expression is exactly divisible by $(x-1)$.

Ex. 3. *Find the quotient and the remainder, when*

(*i*) $(3x^7 - x^6 + 31x^4 + 21x + 5)$ *is divided by* $(x+2)$.

(*ii*) $(x^4 + 5x^3 + 4x^2 + 8x - 20)$ *is divided by* $(x-1)$.

(*iii*) $(x^3 + 2x^2 - 3x - 4)$ *is divided by* $(2x-1)$.

(*i*) Here the multiplier is (–2) and we have

–2	3	–1	0	31	0	0	21	5
		–6	14	–28	–6	12	–24	6
	3	–7	14	3	–6	12	–3	11

The quotient is $(3x^6 - 7x^5 + 14x^4 + 3x^3 - 6x^2 + 12x - 3)$ and the remainder is 11.

(*ii*) Here the multiplier is 1 and we have

1	1	5	4	8	–20
		1	6	10	18
	1	6	10	18	–2

The quotient is $(x^3 + 6x^2 + 10x + 18)$ and the remainder is (–2).

(*iii*) Here we first divide by $(x - \frac{1}{2})$ as under :

$\frac{1}{2}$	1	2	–3	–4
		$\frac{1}{2}$	$\frac{5}{4}$	$-\frac{7}{8}$
	1	$\frac{5}{2}$	$-\frac{7}{4}$	$-\frac{39}{8}$

The required quotient is $\frac{1}{2}\left(x^2 + \frac{5}{2}x - \frac{7}{4}\right)$ and the remainder is $\left(-\frac{39}{8}\right)$.

Ex. 4. *Express* $f(x) = x^5 + 5x^3 + 3x$ *as a polynomial in* $(x-1)$.

Also find $f(x+1)$.

Let us divide $(x^5 + 5x^3 + 3x)$ by $(x-1)$ by synthetic method in succession.

1	1	0	5	0	3	0
		1	1	6	6	9
	1	1	6	6	9	9
		1	2	8	14	
	1	2	8	14	23	
		1	3	11		
	1	3	11	25		
		1	4			
	1	4	15			
		1				
	1	5				

Hence $f(x) = x^5 + 5x^3 + 3x$

$= (x-1)^5 + 5(x-1)^4 + 15(x-1)^3 + 25(x-1)^2 + 23(x-1) + 9$.

Also $f(x+1) = x^5 + 5x^4 + 15x^3 + 25x^2 + 23x + 9$.

Alternatively, using Taylor's finite expansion of $f(x+1)$, we have

$$f(x+1) = f(x) + f'(x) + \frac{1}{2!}f''(x) + \frac{1}{3!}f'''(x) + \frac{1}{4!}f^{iv}(x) + \frac{1}{5!}f^{v}(x),$$

since $h = 1$ here

$$= x^5 + 5x^3 + 3x + 5x^4 + 15x^2 + 3 + \frac{1}{2}(20x^3 + 30x)$$

$$+ \tfrac{1}{6}(60x^2 + 30) + \tfrac{1}{24}.120x + \frac{1}{120}.120$$

$$= x^5 + 5x^4 + 15x^3 + 25x^2 + 23x + 9.$$

Ex. 5. *Find a relation between a and b in order that* $(2x^4 - 7x^3 + ax + b)$ *may be exactly divisible by* $(x-3)$.

If the given expression be exactly divisible by $(x-3)$, then $f(3)$ must be zero, where $f(x) = 2x^4 - 7x^3 + ax + b$.

This gives $-27 + 3a + b = 0$, that is, $3a + b = 27$.

Ex. 6. *If* $(ax^3 + bx^2 + cx + d)$ *be divisible by* $(x^2 + l^2)$, *then show that* $ad = bc$.

Here $(x^2 + l^2)$ is a factor of $(ax^3 + bx^2 + cx + d)$.

Let $ax^3 + bx^2 + cx + d = (x^2 + l^2)(ax + p)$, where p is constant

$$= ax^3 + px^2 + al^2x + l^2p.$$

Therefore $b = p$, $c = al^2$ and $d = l^2p$. Hence $ad = al^2p = bc$.

Examples II (A)

1. If $f(x) = 2x^3 + 5x^2 - 4x - 2$, then find

(*i*) $f(0)$. (*ii*) $f(2)$. (*iii*) $f(-3)$. (*iv*) $f(\sqrt{2})$. (*v*) $f(1.5)$.

2. Find the remainder, when

(*i*) $(3x^2 + 4x - 11)$ is divided by $(x-1)$.

(*ii*) $(2x^3 - 3x + 2)$ is divided by $(x+2)$.

(*iii*) $(x^5 - 4x^4 + 7x^3 - 11x - 13)$ is divided by $(x-2)$.

(*iv*) $(3x^4 + 5x^3 - 2x^2 + 4x + 6)$ is divided by $(x-1)$.

(*v*) $(x^4 + 4x^2 - 9x + 21)$ is divided by $(2x-7)$.

(*vi*) $(3x^4 - 4x^3 + 2x^2 - 9x + 1)$ is divided by $(2x+1)$.

3. Show that $(x^4 - 16x^3 + 86x^2 - 176x + 105)$ is exactly divisible by $(x-3)$.

4. Show that $(x^4 + 2x^3 - 13x^2 - 14x + 24)$ is exactly divisible by $(x+4)$.

5. Find a relation between a and b, if $(4x^3 - 3x^2 + 2ax + b)$ be exactly divisible by $(x+2)$.

6. Find a relation between a and b, if $(ax^5 + 3x^3b + 8)$ be exactly divisible by $(x-2)$.

7. Find the quotient polynomial and the remainder, when

(i) $(x^3 + 5x^2 + 3x + 2)$ is divided by $(x-1)$.

(ii) $(x^4 + 5x^3 + 4x^2 + 8x - 2)$ is divided by $(x+2)$.

(iii) $(2x^4 + 3x^3 - 9x^2 + 2x - 5)$ is divided by $(x+3)$.

(iv) $(3x^4 - x^3 + 2x^2 - 2x - 1)$ is divided by $(x-3)$.

(v) $(3x^4 + 4x^3 + 7x^2 + 8x - 8)$ is divided by $(3x+1)$.

(vi) $(3x^4 - 4x^3 + 2x^2 - 9x + 1)$ is divided by $(2x-1)$.

8. Express

(i) $(3x^3 - 4x^2 + 5x + 6)$ as a polynomial in $(x+1)$.

(ii) $(x^4 - x^3 + 2x^2 - 3x + 1)$ as a polynomial in $(x-3)$.

(iii) $(3x^4 + 5x^3 - 2x^2 + 4x + 6)$ as a polynomial in $(x-1)$.

(iv) $(4x^5 - 6x^4 + 3x^3 - 5x + 2)$ as a polynomial in $(x+2)$.

(v) $(x^3 + 2x^2 + x + 80)$ as a polynomial in $(x + \frac{1}{3})$. [N.B.H. 2003]

9. (a) If $f(x) = x^4 - 3x^3 + 4x^2 - 5x - 9$, then show that
$f(x+2) = x^4 + 5x^3 + 10x^2 + 7x - 11$.

(b) If $f(x) = 2x^4 - x^3 - 2x^2 + 5x - 1$, then show that
$f(x+3) = 2x^4 + 23x^3 + 97x^2 + 182x + 131$.

10. (a) Find the quotient and the remainder, when
$(x^5 - 5x^4 + 9x^3 - 6x^2 - 16x + 13)$ is divided by $(x^2 - 3x + 2)$.

[The remainder will be a linear function of x.

Let the given polynomial be $f(x) = (x^2 - 3x + 2)Q + A(x-1) + B(x-2)$, since $x^2 - 3x + 2 = (x-1)(x-2)$.

Here Q is the quotient and $\{A(x-1) + B(x-2)\}$ is the remainder.]

(b) Find the remainder when $(x^5 - 3x^4 + 4x^2 + x + 4)$ is divided by $(x+1)(x-2)$. [N.B.H. 2007]

(c) Let $f(x)$ be a polynomial and $a \neq b$ be two real numbers. Show that the remainder in the division of $f(x)$ by $(x-a)(x-b)$ is

$$\frac{(x-b)f(a) - (x-a)f(b)}{a-b}.$$ [K.H. 2012]

11. (*a*) Show that (x^2+x+1) is a factor of $(x^{14}+x^7+1)$.

[Use $x^2+x+1=(x-\omega)(x-\omega^2)$.]

(*b*) Show that (x^2-x+1) is a factor of $(x^{20}+x^{10}+1)$.

(*c*) Show that $(x^{40}+x^{23}+x^{30}+x^{13})$ is divisible by (x^2+1).

12. (*a*) If $(x^3+3px+q)$ has a factor of the form $(x-a)^2$, then show that

$$q^2+4p^3=0.$$

(*b*) If (x^2+px+1) be a factor of (ax^3+bx+c), then show that (x^2+px+1) is also a factor of (cx^3+bx^2+a) and that $a^2-c^2=ab$.

(*c*) If (x^4+px^2+qx+r) has a factor of the form $(x-\alpha)^3$, then show that $8p^3+27q^2=0$ and $p^2+12r=0$. [*C.H. 2009*]

13. If $\{ax^3+3bx^2+3cx+d+k(x-p)^3\}$ be a perfect cube, then show that $(ac-b^2)p^2+(ad-bc)p+(bd-c^2)=0$.

14. Find a cubic in x which shall vanish when $x=1$ and $x=-2$ and shall have the values 4 and 8 when $x=-1$ and $x=2$ respectively.

15. (*a*) Express x^4 and (x^4+3x^3-5x+2) in the form

$$a+bx+cx(x-1)+dx(x-1)(x-2)+ex(x-1)(x-2)(x-3).$$

[First divide the polynomials by x, the quotient by $(x-1)$, the next quotient by $(x-2)$ and the last quotient by $(x-3)$. The successive remainders are the values of a, b, c, d, e.]

(*b*) Show that the polynomial $(2x^3-3x^2-36x+12)$ has a maximum value 56 and a minimum value (-69).

16. (*a*) If two zeros of $(x^4-16x^3+86x^2-176x+105)$ be 1 and 7, then find the other zeros.

(*b*) Form the polynomial whose zeros are $1,-2,3,-4$

Answers

1. (*i*) -2. (*ii*) 26. (*iii*) 1. (*iv*) 8. (*v*) 10.

2. (*i*) -4. (*ii*) -8. (*iii*) -11. (*iv*) 16. (*v*) $\frac{3017}{16}$. (*vi*) $\frac{107}{16}$.

5. $4a-b+44=0$. **6.** $4a+3b+1=0$.

7. (*i*) $Q=x^2+6x+9, R=11$.

(*ii*) $Q=x^3+3x^2-2x+12, R=-26$. (*iii*) $Q=2x^3-3x^2+2, R=-11$.

(*iv*) $Q=3x^3+8x^2+26x+76, R=227$. (*v*) $Q=x^3+x^2+2x+2, R=-10$.

(*vi*) $Q=\frac{1}{2}\left(3x^3-\frac{5}{2}x^2+\frac{3}{4}x-\frac{69}{8}\right), R=-\frac{53}{16}$.

8. (*i*) $3(x+1)^3-13(x+1)^2+22(x+1)-6$.

(*ii*) $(x-3)^4+11(x-3)^3+47(x-3)^2+90(x-3)+64$.

(*iii*) $3(x-1)^4+17(x-1)^3+31(x-1)^2+27(x-1)+16$.

(*iv*) $4(x+2)^5-46(x+2)^4+211(x+2)^3-482(x+2)^2+543(x+2)-236$.

(*v*) $\left(x+\frac{1}{3}\right)^3+\left(x+\frac{1}{3}\right)^2+79\frac{23}{27}$.

10. (*a*) $Q=x^3-2x^2+x+1,\ R=-15x+11$. (*b*) $x+4$.

14. $\frac{4}{3}x^3+\frac{2}{3}x^2-\frac{10}{3}x+\frac{4}{3}$.

15. (*a*) $x^4=0+x+7x(x-1)+6x(x-1)(x-2)+x(x-1)(x-2)(x-3)$;

$x^4+3x^3-5x+2=2-x+16x(x-1)+9x(x-1)(x-2)$
$+x(x-1)(x-2)(x-3)$.

16. (*a*) 3, 5. (*b*) $x^4+2x^3-13x^2-14x+24$.

2.9. Equations and fundamental theorems.

The statement that two polynomials are equal or that a polynomial is equal to zero for certain value or values of the variable is known as *equation.* The particular value or values for which the equality holds are called the *roots* of the equation while the process of finding the roots is known as solution of equation. The *degree* of the equation is the highest power of the variable.

A *complete* equation contains all the lower degree terms beginning from the highest ; otherwise it is an incomplete equation.

The *fundamental theorem* of algebra states that *every algebraic equation has at least one root, real or imaginary*. The proof of this theorem is beyond the scope of this book, but assuming this to be true we deduce certain theorem as its consequence.

Theorem. *Every algebraic equation of degree n has exactly n roots.*

Let $f(x)\equiv a_0x^n+a_1x^{n-1}+\cdots\cdots+a_{n-1}x+a_n=0,\ a_0\neq 0$, be an equation of degree n. By the fundamental theorem, it will have a root, say α_1, such that $f(\alpha_1)=0$.

Then, by the remainder theorem, $f(x)$ will contain a factor of the form $(x-\alpha_1)$. If $f_1(x)$ be the quotient when $f(x)$ is divided by $(x-\alpha_1)$, then $f_1(x)$ must be of degree $(n-1)$ and we can write the equation as

$$f(x)\equiv(x-\alpha_1)f_1(x)=0.$$

Again the equation $f_1(x)=0$ must have a root, say α_2, and can be written as $(x-\alpha_2)f_2(x)=0$, where $f_2(x)$ is a polynomial of degree $(n-2)$.

Thus the given equation can be written as

$$f(x) \equiv (x-\alpha_1)(x-\alpha_2) f_2(x) = 0 .$$

Proceeding in this way, we notice that after each factor of $f(x)$, the degree of the quotient polynomial is diminished by one. Hence we shall have ultimately n linear factors of the form $(x-\alpha_1),(x-\alpha_2),.....,(x-\alpha_n)$ and the equation can be put in the form

$$a_0(x-\alpha_1)(x-\alpha_2)(x-\alpha_3).....(x-\alpha_n) = 0 .$$

Now the equality holds for any one of the n values of

$$x = \alpha_1, \alpha_2, ..., \alpha_n ;$$

for, the corresponding factor on the left becomes zero.

Thus every equation of n-th degree will have n roots.

Next suppose that the equation $f(x) = 0$ has a root α different from any one of the above n roots. Then α will satisfy the above equation and hence we can write

$$f(\alpha) \equiv a_0(\alpha-\alpha_1)(\alpha-\alpha_2)(\alpha-\alpha_3).....(\alpha-\alpha_n) = 0 .$$

But, by hypothesis, $a_0 \neq 0$ and α being not equal to any one of $\alpha_1, \alpha_2, ..., \alpha_n$, none of the factors

$$(\alpha-\alpha_1),(\alpha-\alpha_2),.....,(\alpha-\alpha_n)$$

is zero. This implies that $f(\alpha)$ cannot be zero and α is not a root.

Thus the equation cannot have more than n roots.

Note. If an equation of n-th degree be satisfied by more than n distinct values of the variable, then it is an *identity*.

Some of the roots of an equation may be equal and we say the equation to have multiple roots. If r of the n roots be equal, then r is the order of multiplicity and $f(x)$ contains $(x-\alpha_1)^r$ as a factor, if α_1 be the equal root.

2.10. Nature of the roots of an equation.

(a) In an equation with rational coefficients, irrational roots occur in conjugate pairs.

Consider the polynomial $f(x)$ of degree $n(\geq 2)$ and divide it by the product

$\left\{x-\left(\alpha+\sqrt{\beta}\right)\right\}\left\{x-\left(\alpha-\sqrt{\beta}\right)\right\}$, which is $\left\{(x-\alpha)^2-\beta\right\}$.

Now, when the polynomial $f(x)$ is divided by $\left\{(x-\alpha)^2-\beta\right\}$, the quotient $Q(x)$, say, will be of degree $(n-2)$ and the remainder will be at best of degree one.

Thus we can write

$$f(x)=\left\{x-\left(\alpha+\sqrt{\beta}\right)\right\}\left\{x-\left(\alpha-\sqrt{\beta}\right)\right\}Q(x)+Rx+R', \quad \ldots \quad (1)$$

$(Rx+R')$ being the remainder, where R and R' are rational.

Now, if $\left(\alpha+\sqrt{\beta}\right)$ be a root of the equation $f(x)=0$, then substituting $\left(\alpha+\sqrt{\beta}\right)$ for x in (1), we get, since $f\left(\alpha+\sqrt{\beta}\right)=0$,

$$R\left(\alpha+\sqrt{\beta}\right)+R'=0, \quad \text{that is,} \quad (R\alpha+R')+R\sqrt{\beta}=0.$$

Equating the rational and the irrational parts separately to zero, we get $R\alpha+R'=0$ and $R=0$, since $\beta\neq 0$. Therefore $R=R'=0$.

Hence (1) reduces to

$$f(x)=\left\{x-\left(\alpha+\sqrt{\beta}\right)\right\}\left\{x-\left(\alpha-\sqrt{\beta}\right)\right\}Q(x),$$

suggesting that $f(x)=0$ for $x=\alpha-\sqrt{\beta}$ too.

Hence $\left(\alpha-\sqrt{\beta}\right)$ is another root of the equation $f(x)=0$, if $\left(\alpha+\sqrt{\beta}\right)$ be a root.

(b) In an equation with real coefficients, imaginary roots occur in conjugate pairs.

Consider the polynomial $f(x)$ of degree $n(\geq 2)$ and divide it by the product

$$\left\{x-\left(\alpha+i\beta\right)\right\}\left\{x-\left(\alpha-i\beta\right)\right\}, \text{ which is } \left\{(x-\alpha)^2+\beta^2\right\}.$$

Now, when the polynomial $f(x)$ is divided by

$$\left\{(x-\alpha)^2+\beta^2\right\},$$

the quotient $Q(x)$, say, will be of degree $(n-2)$ and the remainder will be at best of degree one. Thus we can write

$$f(x)=\left\{x-\left(\alpha+i\beta\right)\right\}\left\{x-\left(\alpha-i\beta\right)\right\}Q(x)+Rx+R', \quad \ldots \quad (1)$$

$(Rx+R')$ being the remainder, where R and R' are real.

Now, if $\left(\alpha+i\beta\right)$ be a root of the equation $f(x)=0$, then substituting $\left(\alpha+i\beta\right)$ for x in (1), we get, since $f\left(\alpha+i\beta\right)=0$,

$$R\left(\alpha+i\beta\right)+R'=0$$

or, $$(R\alpha+R')+iR\beta=0.$$

Equating the real and the imaginary parts separately to zero, we get

$$R\alpha+R'=0 \text{ and } R=0, \text{ since } \beta\neq 0.$$

Therefore $$R=R'=0.$$

Hence (1) reduces to $f(x)=\{x-(\alpha+i\beta)\}\{x-(\alpha-i\beta)\}Q(x)$, suggesting that $f(x)=0$ for $x=\alpha-i\beta$ too.

Hence $(\alpha-i\beta)$ is another root of the equation $f(x)=0$, if $(\alpha+i\beta)$ be a root.

Note. The occurrence of irrational or imaginary roots in an algebraic equation of multiplicity m, ensures the occurrence of the conjugate irrational or imaginary roots of the same multiplicity.

2.11. General properties of equations.

(a) If two real quantities α and β be substituted for the variable x in any polynomial $f(x)$ with real coefficients and if they give results having opposite signs, then the equation $f(x)=0$ must have at least one real root intermediate in value between α and β.

A polynomial $f(x)$ being a continuous function of x changes continuously from $f(\alpha)$ to $f(\beta)$ as the variable x changes gradually from α to β and hence it passes through all intermediate values. Again, since $f(\alpha)$ and $f(\beta)$ are of contrary signs, it follows that for some value of x, intermediate between α and β, $f(x)$ vanishes and we get a root of the equation $f(x)=0$ there.

(b) (i) If $f(\alpha)$ and $f(\beta)$ be of opposite signs, then the equation $f(x)=0$ has an odd number of real roots between α and β.

(ii) If $f(\alpha)$ and $f(\beta)$ be of the same sign, then the equation $f(x)=0$ has no real root or an even number of real roots between α and β.

(i) Let $\beta>\alpha$ and the degree of the equation be n. Let $\alpha_1,\alpha_2,.....,\alpha_r$ be the $r(r<n)$ real roots of $f(x)=0$ between α and β. Let $\phi(x)$ be the quotient when $f(x)$ is divided by the product $(x-\alpha_1)(x-\alpha_2).....(x-\alpha_r)$, so that

$$f(x)\equiv(x-\alpha_1)(x-\alpha_2).....(x-\alpha_r)\,\phi(x). \quad ... \quad (1)$$

Since $\alpha_1,\alpha_2,.....,\alpha_r$ are all the roots of $f(x)=0$ lying between α and β, $\phi(\alpha)$ and $\phi(\beta)$ must have the same sign, as $\phi(x)=0$ cannot have any real root between α and β.

Putting successively α and β for x in (1), we get

$$f(\alpha)=(\alpha-\alpha_1)(\alpha-\alpha_2).....(\alpha-\alpha_r)\,\phi(\alpha),$$

$$f(\beta)=(\beta-\alpha_1)(\beta-\alpha_2).....(\beta-\alpha_r)\,\phi(\beta).$$

Now, since $\alpha < \alpha_1, \alpha_2, ..., \alpha_r < \beta$,
the factors $(\alpha-\alpha_1),(\alpha-\alpha_2),.....,(\alpha-\alpha_r)$ are all negative and the factors $(\beta-\alpha_1),(\beta-\alpha_2),.....,(\beta-\alpha_r)$ are all positive.

Now $f(\alpha)$ and $f(\beta)$ are of opposite signs while $\phi(\alpha)$ and $\phi(\beta)$ are of same sign. Therefore

$$(\alpha-\alpha_1)(\alpha-\alpha_2).....(\alpha-\alpha_r) \quad \ldots \quad (2)$$

and
$$(\beta-\alpha_1)(\beta-\alpha_2).....(\beta-\alpha_r) \quad \ldots \quad (3)$$

must have opposite signs, if and only if the number of factors be odd leading to the existence of an odd number of real roots of the equation $f(x)=0$ between α and β.

(*ii*) If $f(\alpha)$ and $f(\beta)$ have the same sign, procedding as before, we can conclude that the products (2) and (3) must have the same sign, which is possible, if and only if the number of factors be either nil or even, leading to the existence of no real root or an even number of real roots between α and β.

(*c*)(*i*) *An equation of an odd degree must have at least one real root, opposite in sign to that of the last term (that is, the constant term), the leading term being positive.*

(*ii*) *An equation of an even degree, whose last term (that is, the constant term) is negative, has at least two real roots, one positive and the other negative.*

Let the equation of n-th degree be

$$f(x) \equiv a_0x^n + a_1x^{n-1} + \cdots\cdots + a_{n-1}x + a_n = 0.$$

(*i*) Let n be odd and a_0 be positive. Then

$$f(-\infty) = \text{ negative},$$

$$f(0) = a_n,$$

$$f(\infty) = \text{ positive}.$$

If a_n be positive, then a root of the equation $f(x)=0$ lies between $(-\infty)$ and 0 which is negative; if a_n be negative, then a root of $f(x)=0$ lies between 0 and ∞ which is positive.

(*ii*) In this case, n is even and a_n is negative.

We have $f(-\infty) =$ positive,

$f(0) = a_n$, a negative quantity,

$f(\infty) =$ positive.

Thus there is at least one real root between $(-\infty)$ and 0 and at least one real root between 0 and ∞, the former is negative while the latter is positive.

2.12. Multiple roots.

Let $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the roots of the equation $f(x)=0$ of degree n. Let the first $r(r<n)$ quantities of them be equal to α_1; then we can write

$$f(x)=(x-\alpha_1)^r \phi(x),\ \phi(\alpha_1)\neq 0,$$

and we say that α_1 is a root of the equation $f(x)=0$ of multiplicity r.

Also α_1 is said to be a *zero of order r* of the polynomial $f(x)$.

Theorem. If α_1 *be a root of the equation* $f(x)=0$ *of multiplicity r, then* α_1 *is a root of the equation* $f'(x)=0$ *of multiplicity* $(r-1)$, *where* $f'(x)$ *is the first derived function of* $f(x)$.

We have $f(x)=(x-\alpha_1)^r \phi(x), \phi(\alpha_1)\neq 0$.

Therefore $f'(x)=r(x-\alpha_1)^{r-1}\phi(x)+(x-\alpha_1)^r \phi'(x)$

$$=(x-\alpha_1)^{r-1}\{r\phi(x)+(x-\alpha_1)\phi'(x)\}.$$

Hence $(x-\alpha_1)^{r-1}$ is a common factor of $f(x)$ and $f'(x)$.

This proves the theorem.

Cor.1. If α_1 be a root of the equation $f(x)=0$ of multiplicity r_1 and α_2 be a root of the equation of multiplicity r_2, then α_1 is a root of the equation $f'(x)=0$ of multiplicity (r_1-1) and α_2 is a root of the equation $f'(x)=0$ of multiplicity (r_2-1).

Cor.2. Any root of the equation $f(x)=0$ of multiplicity r occurs in degrees of multiplicity diminishing by unity in the first $(r-1)$ derived equations.

Cor.3. If $f(x)$ and its first $(m-1)$ derived functions all vanish for $x=\alpha$, then $(x-\alpha)^m$ is a factor of $f(x)$ and vice-versa.

Note. In order to obtain the multiple roots of the equation $f(x)=0$, we first find the highest common factor of $f(x)$ and $f'(x)$. Then the common factor will give multiple roots of the equation by the next higher multiplicity.

2.13. Rolle's theorem.

Between any two consecutive real roots of the equation $f(x)=0$ *with real coefficients, there lies at least one real root or an odd number of real roots of the equation* $f'(x)=0$.

Let α, β be two consecutive roots of the equation $f(x)=0$ of multiplicity m and n respectively, so that

$$f(x) \equiv (x-\alpha)^m (x-\beta)^n \phi(x),$$

where $\phi(\alpha) \neq 0$ and $\phi(\beta) \neq 0$. These imply that $\phi(x)$ maintains the same sign for all x between α and β.

Taking logarithmic differentiation, we have

$$\frac{f'(x)}{f(x)} = \frac{m}{x-\alpha} + \frac{n}{x-\beta} + \frac{\phi'(x)}{\phi(x)}.$$

Hence $f'(x) = (x-\alpha)^{m-1} (x-\beta)^{n-1} \left[\{m(x-\beta)+n(x-\alpha)\} \phi(x) + (x-\alpha)(x-\beta) \phi'(x) \right]$

$$= (x-\alpha)^{m-1} (x-\beta)^{n-1} F(x), \text{ say,}$$

where $F(x) = \{m(x-\beta)+n(x-\alpha)\} \phi(x) + (x-\alpha)(x-\beta) \phi'(x)$.

Now putting successively $x = \alpha, \beta$, we get

$$F(\alpha) = m(\alpha-\beta) \phi(\alpha) \text{ and } F(\beta) = n(\beta-\alpha) \phi(\beta).$$

But, since $\phi(\alpha)$ and $\phi(\beta)$ are of the same sign, $F(\alpha)$ and $F(\beta)$ must be of opposite signs. Hence the equation $F(x)=0$ must have at least one root or an odd number of roots between α and β.

Therefore the equation $f'(x)=0$ has at least one real root or an odd number of real roots between α and β.

Cor. 1. If all the roots of an equation $f(x)=0$ be real and distinct, then all roots of the equation $f'(x)=0$ are also real and distinct and these are different from the roots of the equation $f(x)=0$.

Let the equation $f(x)=0$ have n real and distinct roots.

Between any two consecutive roots, there lies only one root of the equation $f'(x)=0$ and no more ; for, the number of roots of the equation $f'(x)=0$ is $(n-1)$.

Cor. 2. Between any two consecutive real roots of the equation $f'(x)=0$, there can lie only one (but not more than one) real root of the equation $f(x)=0$.

Let α and β be two roots of the equation $f(x)=0$ lying between two consecutive real roots of the equation $f'(x)=0$. Then between α and β there must lie a root of the equation $f'(x)=0$ which is contrary to the hypothesis.

Cor. 3. The equation $f(x)=0$ cannot have more than one real root greater than the greatest root of the equation $f'(x)=0$ and the equation $f(x)=0$ cannot have more than one real root less than the least root of the equation $f'(x)=0$.

Cor. 4. If the equation $f'(x)=0$ has r real roots, then the equation $f(x)=0$ cannot have more than $(r+1)$ real roots. Conversely, if the equation $f(x)=0$ has r real roots, then the equation $f'(x)=0$ has at least $(r-1)$ real roots.

2.14. Descartes' rule of signs.

An equation $f(x)=0$ with real coefficients cannot have more positive roots than there are changes of sign in $f(x)$ and cannot have more negative roots than there are changes of sign in $f(-x)$. If the number of real roots be less than the number of changes of sign, then it will be by an even number.

First of all, we show that when a polynomial is multiplied by a binomial of the form $(x-\alpha)$ whose signs are $+-$, there will be at least one more change of sign in the product than in the original polynomial. Let the signs of the terms in a polynomial be

$$++--+---+-.$$

Writing down the signs only of the terms in the multiplication, we have

$$\begin{array}{l} ++--+---+- \\ \underline{+-\qquad\qquad\qquad\quad} \\ ++--+---+- \\ \quad --+-+++-+ \\ \underline{\qquad\qquad\qquad\quad} \\ +\pm-\mp+-\mp\mp+-+ \end{array}$$

Thus we see that in the product

(*i*) an ambiguity replaces each continuation of sign in the original polynomial;

(*ii*) the signs before and after an ambiguity or set of ambiguities are unlike;

(*iii*) a change of sign is introduced at the end.

Let us consider the most unfavourable case and suppose that all the ambiguities are replaced by continuations; from (*ii*), we see that the number of changes of sign will be the same whether we take the upper or the lower sign. Let us take the upper. Thus the number of changes of sign cannot be less than in

$$++--+---+-+$$

and this series of signs is the same as in the original polynomial with an additional change of sign at the end.

If then we suppose that the factors corresponding to the negative (namely, $x+\beta$) and imaginary (namely, $x-\gamma-i\delta$) roots to be already multiplied together to form a polynomial with no change or certain changes of signs of terms, each factor $(x-\alpha)$, corresponding to a positive root introduces at least one change of sign in the product polynomial. Thus no equation can have more positive roots than it has changes of sign.

We assumed earlier that the polynomial is complete ; if some of the coefficients be zero, it will be seen still then that no changes of sign are lost.

Again the roots of the equation $f(-x)=0$ are equal to those of the equation $f(x)=0$ but opposite to them in sign. Therefore the negative roots of the equation $f(x)=0$ are the positive roots of the equation $f(-x)=0$. But the number of these positive roots cannot exceed the number of changes of sign in $f(-x)$; that is, the number of negative roots of the equation $f(x)=0$ cannot exceed the number of changes of sign in $f(-x)$.

Cor. 1. If the signs of the terms of an equation be all positive, then it cannot have a positive root.

Cor. 2. If the signs of the terms of a complete equation be alternately positive and negative, then it cannot have a negative root.

Cor. 3. If an equation involves only even powers of x and if all the coefficients have positive signs, then it cannot have any real root.

Cor. 4. If an equation involves only odd powers of x and if all the coefficients have positive signs, then it has the root zero and no other real root.

Cor. 5. If the roots of a complete equation $f(x)=0$ be all real, then the number of positive roots is equal to the number of variations of sign in $f(x)$ and that of its negative roots is equal to the number of variations of sign in $f(-x)$.

Note. Descartes' rule of signs determines only a maximum limit of the number of positive or negative roots of an equatiom and not the actual number. If it be such that the sum of the greatest possible number of positive roots added to the greatest possible number of negative roots is less than the degree of the equation, then there will be imaginary roots of the equation. If the degree of the equation be n and $f(x)$ has p changes of sign while $f(-x)$ has q changes of sign, then the least number of imaginary roots of $f(x)=0$ is $(n-p-q)$. The number of positive real roots of the equation is $f(x)=0$ either equal to p or less than p by an even number. The number of negative real roots of the equation $f(x)=0$ is either equal to q or less than q by an even number. The number of imaginary roots of the equation $f(x)=0$ is either equal to $(n-p-q)$ or greater than $(n-p-q)$ by an even number.

2.15. Illustrative Examples.

Ex. 1. *Find the equation whose roots are* $1, -2, 3, -4$.

The equation whose roots are $1, -2, 3, -4$ is

$(x-1)(x+2)(x-3)(x+4)=0$, that is, $(x^2+x-2)(x^2+x-12)=0$

or, $(x^2+x)^2-14(x^2+x)+24=0$

or, $x^4+2x^3-13x^2-14x+24=0$.

Ex. 2. *Find the value of* $(x^3-7x^2-2x+88)$ *when* $x=5+i\sqrt{3}$.

The equation whose roots are $(5+i\sqrt{3})$ and $(5-i\sqrt{3})$ is

$$(x-5-i\sqrt{3})(x-5+i\sqrt{3})=x^2-10x+28=0.$$

Hence the value of $(x^2-10x+28)$ is zero when $x=5+i\sqrt{3}$.

The given expression $=x(x^2-10x+28)+3(x^2-10x+28)+4$

$=x\times 0+3\times 0+4$ when $x=5+i\sqrt{3}$

$=4$.

Ex. 3. *Solve the equation* $x^4-3x^3-5x^2+9x-2=0$, $(2-\sqrt{3})$ *being one of its roots.*

The coefficients of the given equation are all rational numbers. Hence, if $(2-\sqrt{3})$ be a root of the equation, then $(2+\sqrt{3})$ must also be a root.

Therefore $(x-2-\sqrt{3})(x-2+\sqrt{3})=(x-2)^2-3=x^2-4x+1$ is a factor of $(x^4-3x^3-5x^2+9x-2)$.

Dividing by the factor, we get the reduced equation as

$$x^2+x-2=0, \text{whence } x=1,-2.$$

Thus the roots of the given equation are $1, -2, 2\pm\sqrt{3}$.

Ex. 4. *Show that the roots of the equation*

$$\frac{1}{x-a}+\frac{1}{x-b}+\frac{1}{x-c}=\frac{1}{x}, \text{ where } a>b>c>0, \text{ are real.} \quad [T.H.\ 2009]$$

The given equation may be written as

$$\frac{x}{x-a}+\frac{x}{x-b}+\frac{x}{x-c}=1$$

or, $$\left(\frac{x}{x-a}-1\right)+\left(\frac{x}{x-b}-1\right)+\left(\frac{x}{x-c}-1\right)+2=0$$

or, $$\frac{a}{x-a}+\frac{b}{x-b}+\frac{c}{x-c}+2=0.$$

If possible, let $(\alpha+i\beta)$ be an imaginary root of the equation. Then, since the coefficients of the equation are real, $(\alpha-i\beta)$ is also a root of the equation.

Substituting these values for x, we get

$$\frac{a}{\alpha+i\beta-a}+\frac{b}{\alpha+i\beta-b}+\frac{c}{\alpha+i\beta-c}+2=0 \quad \ldots \quad (1)$$

and $$\frac{a}{\alpha-i\beta-a}+\frac{b}{\alpha-i\beta-b}+\frac{c}{\alpha-i\beta-c}+2=0. \quad \ldots \quad (2)$$

By subtraction,

$$-2i\beta\left\{\frac{a}{(\alpha-a)^2+\beta^2}+\frac{b}{(\alpha-b)^2+\beta^2}+\frac{c}{(\alpha-c)^2+\beta^2}\right\}=0.$$

Since $a, b, c>0$ and α, β are real, the expression within the brackets cannot be zero. Hence $\beta=0$.

Thus there is no imaginary root of the equation and the roots are all real.

Ex. 5. *Show that the equation* $x^3-3x^2-9x+27=0$ *has a multiple root.*

Let $f(x)=x^3-3x^2-9x+27$.

Therefore $f'(x)=3x^2-6x-9=3(x^2-2x-3)$.

The highest common factor of $f(x)$ and $f'(x)$ is $(x-3)$.

Therefore $x=3$ is a root of the equation $f'(x)=0$.

Hence the equation $f(x)=0$ has a root 3 of multiplicity 2.

Ex. 6. *Prove that the equation* $x^3+x^2-5x-1=0$ *has one positive root lying in* $(1, 2)$ *and two negative roots lying in* $(-1, 0)$ *and* $(-3, -2)$.

Let $f(x)=x^3+x^2-5x-1$.

Therefore $f(-3)=-27+9+15-1=-4$; $f(-2)=-8+4+10-1=5$;

$f(-1)=-1+1+5-1=4$; $f(0)=-1$;

$f(1)=1+1-5-1=-4$; $f(2)=8+4-10-1=1$.

Now $f(-3)$ and $f(-2)$ are of opposite signs and hence there is at least one negative root between (-3) and (-2). Similarly, from the other results of substitution, it may be said that there is at least one negative root in $(-1, 0)$ and at least one positive root in $(1, 2)$. Since the degree of the equation is 3, it has three roots lying one in each of

$$(-3, -2), (-1, 0) \text{ and } (1, 2).$$

Ex. 7. *Apply Descartes' rule of signs to find the nature of the roots of the equation* $x^4+16x^2+7x-11=0$.

Let $f(x)=x^4+16x^2+7x-11.$

There is only one change of sign in $f(x)$. Hence there cannot be more than one positive real root of the equation $f(x)=0$ and the number of positive real roots is exactly one.

Again $f(-x) = x^4 + 16x^2 - 7x - 11$.

There is only one change of sign in $f(-x)$. Hence there cannot be more than one negative real root of the equation $f(x) = 0$ and the number of negative real roots is exactly one.

The degree of the equation being even with a negative last term, the other two roots are imaginary.

Thus the equation has one positive real root, one negative real root and two imaginary roots.

Ex. 8. *If p, q, r be positive, then show that $x^4 + px^3 + qx - r = 0$ has one positive, one negative and two imaginary roots.*

Let $f(x) = x^4 + px^3 + qx - r$.

The equation is of even degree with a negative last term.

Since p, q, r are all positive, there is only one change of sign in $f(x)$.
Therefore the equation has only one positive real root.

Again $f(-x) = x^4 - px^3 - qx - r$.

Therefore the equation $f(-x) = 0$ has only one positive real root, that is, the equation $f(x) = 0$ has only one negative real root.

As the degree of the equation is 4, the other two roots are imaginary.

Examples II (B)

1. Find the equation whose roots are $2, -3, 4, -1$.

2. In the equation $x^4 + 2x^3 - 13x^2 - 14x + 24 = 0$ two roots are 1 and (-2); find the others.

3. Form a rational cubic equation which shall have for roots 1 and $(2 + 3i)$.

4. (*a*) Form an equation of degree four with rational coefficients which will have two of its roots as

(*i*) $4 - \sqrt{2}, 2 + i\sqrt{3}$. (*ii*) $2 - 3i, 1 + 5i$. (*iii*) $i, \frac{1}{\sqrt{2}}$.

(*b*) Find the equation of the fourth degree with rational coefficients one root of which is (*i*) $\sqrt{2} + i\sqrt{3}$. (*ii*) $\sqrt{a} + \sqrt{b}$.

5. Solve the equations :

(*i*) $x^3 - 7x^2 + 19x - 13 = 0$, one root being $(3 + 2i)$.

(*ii*) $3x^3 - 4x^2 + x + 88 = 0$, one root being $2 + \sqrt{-7}$. [*B.H. 1973*]

(*iii*) $x^4 - 3x^3 - 5x^2 + 9x - 2 = 0$, one root being $(2 + \sqrt{3})$.

(*iv*) $x^4 + 2x^3 - 5x^2 + 6x + 2 = 0$, one root being $(-2 + \sqrt{3})$.

(*v*) $x^4 - 7x^3 + 14x^2 - 2x - 12 = 0$, one root being $(1 + \sqrt{3})$.

6. (*a*) The equation $x^4 - 16x^3 + 86x^2 - 176x + 105 = 0$ has a root 1; find the equation containing the remaining roots.

(*b*) Find the values of a and b so that $(1+i)$ is a root of the equation $x^4 - ax^3 + bx^2 - 4x + 2 = 0$.

(*c*) Solve the equation $3x^4 - 25x^3 + 50x^2 - 50x + 12 = 0$ having an imaginary root with modulus $\sqrt{2}$. [*U. H. 1968*]

(*d*) Prove that for any real root a of the equation $x^3 - 1 = 0$, ia is a root of the equation $x^{12} - 1 = 0$. [*B. H. 1997*]

(*e*) If $(\alpha + i\beta)$ be a root of the equation $x^3 + qx + r = 0$, then prove that 2α will be a root of the equation $x^3 + qx - r = 0$, $(\beta \neq 0)$. [*T. H. 1991*]

7. (*a*) Show that the equation

$$\frac{A^2}{x-a} + \frac{B^2}{x-b} + \frac{C^2}{x-c} + \cdots\cdots + \frac{L^2}{x-l} = x - m,$$

where $a, b, c, \ldots\ldots, l, m$ are real numbers, all different, cannot have an imaginary root. [*K. H. 2008*]

(*b*) Show that each of the equations

$$\frac{1}{x-1} + \frac{2}{x-2} + \frac{3}{x-3} = \frac{1}{x} \text{ and } \frac{1}{x-1} + \frac{2}{x-2} + \frac{2}{x-3} = \frac{x-6}{2}$$

has all its roots real.

(*c*) Show that the roots of the equations

(*i*) $\dfrac{1}{x-1} + \dfrac{2}{x-2} + \dfrac{3}{x-3} + \dfrac{4}{x-4} = x - 5,$ [*V. H. 2003*]

(*ii*) $\dfrac{1}{x-1} + \dfrac{2}{x-2} + \dfrac{3}{x-3} + \dfrac{4}{x-4} + \dfrac{5}{x-5} = 6,$ [*B. H. 1973*]

(*iii*) $\dfrac{1}{x+a_1} + \dfrac{1}{x+a_2} + \cdots\cdots + \dfrac{1}{x+a_n} = \dfrac{1}{x},$ [*C. H.2009*]

($a_1, a_2, \ldots\ldots, a_n$ being negative real numbers)

are all real.

(*d*) Show that the equation

$(x-a)^3 + (x-b)^3 + (x-c)^3 + (x-d)^3 = 0$, where a, b, c, d are not all equal, has only one real root.

[*V. H. 1988; C. H. 1989; B. H. 1994, 2002*]

[Since the given equation $f(x) = 0$ is of degree 3, it has either only one real root or three real roots. If possible, let there be three real roots and let α, β be two such real roots. Then the equation $f'(x) = 0$ has one real root between α and β. Now show that the discriminant of the equation $f'(x) = 0$ is negative.]

8. Show that the equation $x^3-2x-5=0$ has no negative real root. [C. H. 1978]

9. (*a*) Apply Descartes' rule of signs to find the nature of the roots of the equations :

(*i*) $3x^4+12x^2+5x-4=0$. (*ii*) $x^4+x^2+x-1=0$.

(*iii*) $x^4+qx^2+rx-s=0$, (q, r, s being positive). [B. H. 1969]

(*b*) Apply Descartes' rule of signs to show that the equation $x^4+2x^2-7x-5=0$ has two real roots and two non-real roots.

10. Show that each of the following equations has at least two imaginary roots :

(*i*) $x^5+x^3-2x^2+x-2=0$. (*ii*) $x^4+15x^2+7x-10=0$.

(*iii*) $x^3+7x+6=0$. (*iv*) $x^6-3x^2-x+1=0$.

11. Show that each of the following equations has at least four imaginary roots :

(*i*) $2x^7-x^4+4x^3-5=0$. (*ii*) $4x^7-8x^4+4x^3-7=0$.

(*iii*) $x^{10}-4x^6+x^4-2x-3=0$. (*iv*) $x^7+5x^4-3x+k=0$.

12. (*a*) Find the exact number of real roots of the equation

$$x^6-x^3+2x^2-3x-1=0.$$

(*b*) Find the number of real roots of the equation $x^4-x^2+x-2=0$ by multiplying it by $(x+2)$. [C. H. 2009]

(*c*) Find the nature of the roots of the equations

(*i*) $x^n+1=0$, [N. B. H. 1985] (*ii*) $x^n-1=0$,

when n is even and when n is odd.

(*d*) Show that the equation $1+x+\frac{x^2}{2}+\cdots\cdots+\frac{x^n}{n}=0$ has no real root if n be even and has only one real root if n be odd.

[Here $(x-1)f'(x)=x^n-1$.] [N. B. H. 2003]

13. (*a*) If $a>0$, then prove that the equation $x^4+2x^2+3x-a=0$ has one positive root, one negative root and two complex roots.

(*b*) Show that the equation $x^3-16x^2-x-1=0$ has one and only one positive root. Show that this root is greater than 8.

14. (*a*) Find the number of real roots of the equation

$$2x^5-4x^4-9x-2=0.$$

Also find the pairs of consecutive integers between which they lie.

(*b*) Find the intervals $a<x<a+1$, where a is zero or an integer which contain the real roots of the equation $x^4-12x+5=0$.

[C. H. 1969]

15. Show that the equation

(*i*) $10x^3 - 17x^2 + x + 6 = 0$ has a root between 0 and (-1).

(*ii*) $x^4 - 12x^2 + 12x - 3 = 0$ has a root between (-3) and (-4) and another between 2 and 3.

(*iii*) $x^5 - 5x^3 + 5x + 4 = 0$ has only one real root which is negative and lies in the interval $(-3, -2)$.

16. (*a*) Find the range of the values of k for which the equation $x^4 + 4x^3 - 2x^2 - 12x + k = 0$ has four real and unequal roots.

[*V. H. 1990*]

[Here $f'(x) = 4x^3 + 12x^2 - 4x - 12 = 4(x+3)(x+1)(x-1)$. The roots of $f'(x) = 0$ are $-3, -1, 1$. If the roots of $f(x) = 0$ be real and unequal, they will be separated by the roots of $f'(x) = 0$. Hence one root will be less than (-3), one root will lie between (-3) and (-1), one root will lie between (-1) and 1 and one root will be greater than 1. Therefore $f(-\infty)$ and $f(-3)$ will be of opposite signs, that is, $f(-3)$ will be negative, since $f(-\infty)$ is positive and so on.]

(*b*) Show that the equation $x^3 - 3x + k = 0$ has three distinct real roots, if $-2 < k < 2$.

(*c*) Show that the equation $x^4 - 14x^2 + 24x + k = 0$ has

(*i*) four real and unequal roots, if $-11 < k < -8$,

[*N. B. H. 1988*]

(*ii*) two unequal real roots, if $-8 < k < 117$,

(*iii*) no real root, if $k > 117$.

17. Solve the following equations which have equal roots :

(*i*) $x^4 - 9x^2 + 4x + 12 = 0$.

(*ii*) $x^4 - 6x^3 + 12x^2 - 10x + 3 = 0$.

18. (*a*) Find the multiple root, if any, of the equations

(*i*) $x^3 + x^2 - 16x + 20 = 0$.

(*ii*) $x^3 + 3x^2 - 4 = 0$.

(*iii*) $x^4 + 3x^3 - 7x^2 - 15x + 18 = 0$.

(*b*) Find the multiple root of the equations

(*i*) $x^4 - 2x^3 + 2x - 1 = 0$,

(*ii*) $x^5 - 3x^4 - 5x^3 + 27x^2 - 32x + 12 = 0$

and hence solve the equations.

19. (*a*) Show that the equation of the form

$$\frac{x^4}{4!} + \frac{x^3}{3!} + \frac{x^2}{2!} + x + 1 = 0$$ cannot have a multiple root.

(*b*) Show that the equation $x^4+px^2+q=0$ cannot have three equal roots.

(*c*) Show that the equation $x^n-1=0$ has no multiple root.

(*d*) Show that $x^n+nx^{n-1}+n(n-1)x^{n-2}+\cdots\cdots+n!=0$ cannot have a multiple root. [*K. H. 2001, 2003*]

20. Find the values of k for which the equation $x^5-x^3-2x+k=0$ may have multiple roots.

21. (*a*) Show that the equation $x^5+5px^3+5p^2x+q=0$ will have a pair of equal roots, if $q^2+4p^5=0$.

(*b*) Show that the equation $x^n-nqx+(n-1)r=0$ will have a pair of equal roots, if $q^n=r^{n-1}$. [*B. H. 1973, 1995*]

(*c*) Show that the equation $x^n-px^2+r=0$ will have a pair of equal roots, if $n^n r^{n-2}=4p^n(n-2)^{n-2}$.

22. (*a*) If $\alpha, \beta, \gamma, \ldots\ldots$ be the roots of the equation $x^n+p_1x^{n-1}+p_2x^{n-2}+\cdots\cdots+p_n=0$, then prove that

$$(1+\alpha^2)(1+\beta^2)(1+\gamma^2)\cdots\cdots=(1-p_2+p_4-\cdots\cdots)^2+(p_1-p_3+p_5-\cdots\cdots)^2.$$

[Here $x^n+p_1x^{n-1}+p_2x^{n-2}+\cdots\cdots+p_n\equiv(x-\alpha)(x-\beta)(x-\gamma)\cdots\cdots$.
Put i and $(-i)$ for x in both sides of the identity and then multiply the two.]

(*b*) If $1, \alpha, \beta, \gamma, \ldots\ldots$ be the roots of the equation $x^n-1=0$, then show that $(1-\alpha)(1-\beta)(1-\gamma)\cdots\cdots=n$. [*C. H. 1980, 1985*]

[Here $x^n-1=(x-1)(x-\alpha)(x-\beta)(x-\gamma)\cdots\cdots$
After dividing both sides by $(x-1)$, put $x=1$ in both sides.]

(*c*) If $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be n distinct roots of the equation $x^n-1=0$, then prove that

$(a+b\alpha_1)(a+b\alpha_2)(a+b\alpha_3)\cdots\cdots(a+b\alpha_n)=a^n+(-1)^{n-1}b^n$. [*C. H. 2006*]

23. If $\alpha, \beta, \gamma, \delta$ be the roots of $x^4-x^3+x^2-x+1=0$, then find the values of $(\alpha+1)(\beta+1)(\gamma+1)(\delta+1)$ and $(\alpha^2+4)(\beta^2+4)(\gamma^2+4)(\delta^2+4)$.

24. If a polynomial equation $f(x)=0$, whose coefficients are all real quantities, has for a root the imaginary expression $(\alpha+\beta i)^p$, where α, β are real and p is a positive integer, then show that it must also have for a root the expression $(\alpha-\beta i)^p$. [*C. H. 1977*]

25. (*a*) Let $f(x)=a_0{}^2x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots\cdots+a_n$, where the coefficients $a_0, a_1, a_2, \ldots\ldots, a_n$ are real. If α be greater than any of the real roots of the equation $f(x)=0$, then show that $f(\alpha)$ is positive. [*C. H. 1969*]

(*b*) Let $f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots\ldots+a_n$, where the coefficients $a_0, a_1, a_2, \ldots\ldots, a_n$ are all integers. If the equation $f(x)=0$ has an integral root α, then show that α must be a factor of a_n. If $\frac{p}{q}$ be a root of the equation $f(x)=0$, where p and q are integers prime to each other, then show that p is a factor of a_n and q is a factor of a_0.

[From $f(\alpha)=0$, we get $\alpha(a_0\alpha^{n-1}+a_1\alpha^{n-2}+\ldots\ldots+a_{n-1})=-a_n$.]

(*c*) (*i*) Show that the integer roots of the equation $x^4+6x^3-27x-10=0$ are 2 and (-5), but the equation $x^4+6x^3+3x^2-14x+15=0$ has no integer root.

(*ii*) Show that the only rational root of the equation

$$3x^3-26x^2+34x-12=0 \text{ is } \tfrac{2}{3},$$

but the equation $x^4+6x^3+3x^2-14x-3=0$ has no rational root.

Answers

1. $x^4-2x^3-13x^2+14x+24=0$. 2. $-4, 3$.
3. $x^3-5x^2+17x-13=0$.
4. (*a*) (*i*) $x^4-12x^3+53x^2-112x+98=0$.
   (*ii*) $x^4-6x^3+47x^2-130x+338=0$. (*iii*) $2x^4+x^2-1=0$.
   (*b*) (*i*) $x^4+2x^2+25=0$. (*ii*) $x^4-2(a+b)x^2+(a-b)^2=0$.
5. (*i*) $1, 3\pm2i$. (*ii*) $-\frac{8}{3}, 2\pm\sqrt{-7}$. (*iii*) $2\pm\sqrt{3}, 1, -2$.
   (*iv*) $-2\pm\sqrt{3}, 1\pm i$. (*v*) $3, 2, 1\pm\sqrt{3}$.
6. (*a*) $x^3-15x^2+71x-105=0$. (*b*) $a=3, b=5$. (*c*) $1\pm i, 6, \frac{1}{3}$.
9. (*a*) (*i*) One positive, one negative, two imaginary roots.
   (*ii*) One positive, one negative, two imaginary roots.
   (*iii*) One positive, one negative, two imaginary roots.
12. (*a*) 2. (*b*) 2.
   (*c*) (*i*) No real root when n is even and one real root when n is odd.
   (*ii*) Two real roots when n is even and one real root when n is odd.
14. (*a*) One root each in (2, 3), (0, −1), (−1, −2)
   (*b*) $0<x<1, 2<x<3$.
16. (*a*) $-7<k<9$. 17. (*i*) $2, 2, -1, -3$. (*ii*) $1, 1, 1, 3$.
18. (*a*) (*i*) 2 is a double root.
   (*ii*) (−2) is a double root.
   (*iii*) (−3) is a double root.
   (*b*) (*i*) $1, 1, 1, -1$ (*ii*) $1, 1, 2, 2, -3$.
20. $k=\pm2$. 23. 5 and 205.

3 THEORY OF EQUATIONS (2)

3.1. Relation between roots and coefficients of an equation.

Let $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the n roots of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots\ldots + p_n = 0;$$

so that we have the identity

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots\ldots + p_n$$

$$= (x - \alpha_1)(x - \alpha_2) \ldots\ldots (x - \alpha_n)$$

$$= x^n - S_1 x^{n-1} + S_2 x^{n-2} + \ldots\ldots + (-1)^n S_n,$$

where S_r is the sum of all the products of $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ taken r at a time.

Equating the coefficients of different powers of x on the two sides of the above identity, we get

S_1 = sum of the roots $= \Sigma \alpha_1 = -p_1$;

S_2 = sum of the products of the roots taken two at a time

$= \Sigma \alpha_1 \alpha_2 = p_2$;

S_3 = sum of the products of the roots taken three at a time

$= \Sigma \alpha_1 \alpha_2 \alpha_3 = -p_3$;

.....

.....

S_n = product of all the roots $= \alpha_1 \alpha_2 \ldots\ldots \alpha_n = (-1)^n p_n$.

When the coefficient of x^n in the equation is p_0, different from unity, then to get $S_1, S_2, S_3, \ldots\ldots$, each coefficient of different terms is divided by p_0. In that case,

$$S_1 = -\frac{p_1}{p_0}, S_2 = \frac{p_2}{p_0}, S_3 = -\frac{p_3}{p_0}, \ldots\ldots, p_0 \neq 0.$$

Cor. If α, β and γ be the roots of the cubic

$$a_0 x^3 + a_1 x^2 + a_2 x + a_3 = 0,$$

then $\alpha + \beta + \gamma = -\frac{a_1}{a_0}$, $\alpha\beta + \beta\gamma + \gamma\alpha = \frac{a_2}{a_0}$ and $\alpha\beta\gamma = -\frac{a_3}{a_0}$.

If α, β, γ and δ be the roots of the biquadratic

$$a_0x^4+a_1x^3+a_2x^2+a_3x+a_4=0,$$

then $$\alpha+\beta+\gamma+\delta=-\frac{a_1}{a_0},$$

$$\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta=\frac{a_2}{a_0},$$

$$\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta=-\frac{a_3}{a_0} \text{ and } \alpha\beta\gamma\delta=\frac{a_4}{a_0}.$$

Note. The number of these fundamental relations between the roots and the coefficients of an equation being the same as the number of roots of the equation, they cannot be used to solve the given equation. To give effect to the solution of equations, some other relation connecting the roots must be given.

3.2. Illustrative Examples.

Ex. 1. *Solve the equation* $x^3-3x^2+4=0$, *two of its roots being equal.*

Let the roots of the equation be α, α, β.

Then $2\alpha+\beta=3$ and $\alpha^2+2\alpha\beta=0$.

These give $\alpha=2, \beta=-1$. Thus the roots are $2, 2, -1$.

Ex. 2. *Solve the equation* $x^3-9x^2+23x-15=0$, *whose roots are in A.P.*

Let the roots of the equation be $(\alpha-\delta), \alpha, (\alpha+\delta)$.

Then we have $3\alpha=9$, $3\alpha^2-\delta^2=23$ and $\alpha(\alpha^2-\delta^2)=15$.

These relations give $\alpha=3$ and $\delta=2$.

Thus the roots are 1, 3, 5.

Ex. 3. *If the roots of the equation* $x^3-ax^2+bx-c=0$ *be in harmonic progression, then show that the mean root is* $\frac{3c}{b}$.

Let α, β, γ be the roots of the given equation ;

so that $\frac{1}{\alpha}+\frac{1}{\gamma}=\frac{2}{\beta}$, that is, $\alpha\beta+\beta\gamma=2\alpha\gamma$.

Also $\alpha\beta+\beta\gamma+\gamma\alpha=b$.

Combining these two relations, we have $3\alpha\gamma=b$.

Again we have $\alpha\beta\gamma=c$.

Dividing, we get $\beta=\frac{3c}{b}$.

Ex. 4. *Find the condition that the cubic* $x^3 - px^2 + qx - r = 0$ *should have its roots in G.P.* [*G. H. 1969 ; N. B. H.1985*]

Let the roots of the cubic be $\frac{\alpha}{\rho}, \alpha, \alpha\rho$.

Then $\alpha\left(\frac{1}{\rho} + 1 + \rho\right) = p,$ ... (1)

$\alpha^2\left(\frac{1}{\rho} + \rho + 1\right) = q$ ... (2)

and $\alpha^3 = r.$ ... (3)

Dividing (2) by (1), we have $\alpha = \frac{q}{p}$.

Substituting for α in (3), we get the required condition as $q^3 = p^3 r$.

Ex. 5. *Find the condition that the equation* $x^3 + px^2 + qx + r = 0$ *may have two roots equal but of opposite signs.*

Let the roots of the equation be $\alpha, (-\alpha), \beta$.

Then $\alpha - \alpha + \beta = -p,$ ... (1)

$-\alpha^2 + \alpha\beta - \alpha\beta = q$ ... (2)

and $-\alpha^2\beta = -r.$ ... (3)

From (1), $\beta = -p$.

Substituting in (3), we get $\alpha^2 p = -r$.

Then, from (2), $\frac{r}{p} = q,$ that is , $r = pq$.

This is the required condition.

Ex. 6. *Solve the equation* $4x^4 - 4x^3 - 13x^2 + 9x + 9 = 0$, *given that the sum of two roots is zero.*

Let the roots be $\alpha, -\alpha, \beta, \gamma$.

Then $\alpha - \alpha + \beta + \gamma = 1,$ ... (1)

$\alpha(-\alpha + \beta + \gamma) - \alpha(\beta + \gamma) + \beta\gamma = -\frac{13}{4},$ ... (2)

$-\alpha^2\beta - \alpha^2\gamma + \alpha\beta\gamma - \alpha\beta\gamma = -\frac{9}{4}$ ... (3)

and $-\alpha^2\beta\gamma = \frac{9}{4}.$ ... (4)

From (1), $\beta + \gamma = 1$

Then (2) gives $-\alpha^2 + \beta\gamma = -\frac{13}{4}$

and (3) gives $-\alpha^2\beta - \alpha^2\gamma = -\frac{9}{4}$, that is , $-\alpha^2(\beta + \gamma) = -\frac{9}{4}$, giving $\alpha = \frac{3}{2}$.

(4) then gives $\beta\gamma = -1$.

These give $\beta = \frac{1}{2}(1+\sqrt{5})$, $\gamma = \frac{1}{2}(1-\sqrt{5})$.

Hence the roots are $\frac{3}{2}, -\frac{3}{2}, \frac{1}{2}(1 \pm \sqrt{5})$.

Ex. 7. *If the equation* $x^4 + ax^3 + bx^2 + cx + d = 0$ *has three equal roots, then show that each of them is equal to* $\dfrac{6c-ab}{3a^2-8b}$. [C. H. 1978; B . H. 1995]

Let the roots of the given equation be $\alpha, \alpha, \alpha, \beta$.

Then $3\alpha + \beta = -a$, ... (1)

$3\alpha^2 + 3\alpha\beta = b$, ... (2)

$\alpha^3 + 3\alpha^2\beta = -c$ ... (3)

and $\alpha^3\beta = d$. ... (4)

Eliminating β from (1) and (2), we get

$6\alpha^2 + 3a\alpha + b = 0$. ... (5)

Eliminating β from (1) and (3), we get

$8\alpha^3 + 3a\alpha^2 - c = 0$. ... (6)

From (5) and (6), we get

$3a\alpha^2 + 4b\alpha + 3c = 0$. ... (7)

From (5) and (7), we get, by cross-multiplication,

$$\frac{\alpha^2}{9ac-4b^2} = \frac{\alpha}{3ab-18c} = \frac{1}{24b-9a^2}.$$

Therefore $\alpha = \dfrac{3ab-18c}{24b-9a^2} = \dfrac{6c-ab}{3a^2-8b}$.

Ex. 8. *Solve the equations*

$$x + py + p^2z = p^3, \quad x + qy + q^2z = q^3, \quad x + ry + r^2z = r^3.$$

We notice from the given equations that if we replace p, q, r by t in the given equations, then all the equations take the form

$$x + ty + t^2z = t^3,$$

so that we may say that p, q, r are the roots of the cubic

$$t^3 - zt^2 - yt - x = 0.$$

Hence $z = p + q + r$, $y = -(pq + qr + rp)$ and $x = pqr$.

Examples III(A)

1. Solve the equations

(*i*) $x^3 - 6x^2 + 3x + 10 = 0$,
(*ii*) $x^3 - 9x^2 + 23x - 15 = 0$,
(*iii*) $x^4 + 2x^3 - 21x^2 - 22x + 40 = 0$,

the roots being in A.P. [*C. H. 1976 ; N. B. H. 1987*]

2. Solve the equations

(*i*) $2x^3 - 21x^2 + 42x - 16 = 0$,
(*ii*) $27x^3 + 42x^2 - 28x - 8 = 0$,
(*iii*) $3x^3 - 26x^2 + 52x - 24 = 0$,
(*iv*) $3x^4 - 40x^3 + 130x^2 - 120x + 27 = 0$,

the roots being in G. P.

3. (*a*) Solve the equation $x^3 - 5x^2 - 4x + 20 = 0$, given that two of its roots are equal and of opposite signs.

(*b*) Solve the equations

(*i*) $x^3 - 5x^2 - 16x + 80 = 0$,
(*ii*) $4x^4 + 12x^3 - 25x^2 - 27x + 36 = 0$,

the sum of two roots of each equation being zero.

(*c*) The sum of two roots of the equation

$$x^3 - a_1 x^2 - a_2 x + a_3 = 0$$

is zero ; show that $a_1 a_2 - a_3 = 0$.

4. Solve the equations

(*i*) $x^3 - 7x^2 + 36 = 0$,

(*ii*) $24x^3 + 46x^2 + 9x - 9 = 0$,

one of the roots of each equation being double of another.

5. Solve the equation $2x^3 - x^2 - 22x - 24 = 0$, two of the roots being in the ratio 3 : 4.

6. (*a*) Solve the equation $4x^3 - x^2 - 27x - 18 = 0$, given that two of its roots α and β are connected by the relation $2\alpha + 3\beta = 0$.

(*b*) Solve the equation $x^3 - 7x^2 + 36 = 0$, given that the difference between two of its roots is 5. [*B. H. 1991*]

(*c*) Solve the equation $4x^3 - 24x^2 + 35x - 12 = 0$, when one of its roots is double the sum of the other two. [*K. H. 2001*]

7. (*a*) Solve the equation $2x^3 + x^2 - 5x + 2 = 0$, if two of its roots α and β be connected by the relation $\alpha\beta + 1 = 0$.

(*b*) Find the condition which must be satisfied by the coefficients of the equation $x^3 + px^2 + qx + r = 0$, when two of its roots α and β are connected by the relation $\alpha\beta + 1 = 0$.

8. (*a*) If one of the roots of the equation

$$x^3 + px^2 + qx + r = 0$$

equals the sum of the other two, then prove that $p^3 + 8r = 4pq$.

(*b*) Determine r so that one root of the equation

$$x^3 - rx^2 + rx - 4 = 0$$

shall be reciprocal of another and find the roots.

9. Find the conditions that the roots of the equations

(*i*) $x^3 + px^2 + qx + r = 0$,

(*ii*) $x^4 + ax^3 + bx^2 + cx + d = 0$

are in A.P.

[Take $\alpha - 3\beta, \alpha - \beta, \alpha + \beta, \alpha + 3\beta$ as the roots of (*ii*).]

10. Find the condition that the roots of the equation

$$x^4 + px^3 + qx^2 + rx + s = 0$$

may be in G.P.

[Take $\frac{\alpha}{\beta^3}, \frac{\alpha}{\beta}, \alpha\beta, \alpha\beta^3$ as the roots .]

11. (*a*) If the roots of the equation $x^3 + 3px^2 + 3qx + r = 0$ be in H.P., then show that $2q^3 = r(3pq - r)$.

(*b*) If the roots of the equation $x^3 - ax^2 + x - b = 0$ be in H.P., then show that the mean root is $3b$.

(*c*) Solve the equation $3x^3 - 22x^2 + 48x - 32 = 0$, the roots of which are in harmonic progression. [*B. H. 2001*]

12. If one root of the equation $x^3 + ax + b = 0$ be twice the difference of the other two, then show that one root is $\frac{13b}{3a}$.

13. If the equation $ax^3 + 3bx^2 + 3cx + d = 0$ has two equal roots, then show that $(bc - ad)^2 = 4(b^2 - ac)(c^2 - bd)$ and each of the equal roots is $\frac{bc - ad}{2(ac - b^2)}$.

14. (*a*) Solve the equation $x^4 - 5x^3 + 11x^2 - 13x + 6 = 0$, given that two of its roots α and β are connected by the relation $3\alpha + 2\beta = 7$.

(*b*) Solve the equation $x^4 - 5x^3 + 11x^2 - 13x + 6 = 0$ which has two roots whose difference is 1. [*C. H. 1974*]

15. Solve the equation $x^4+4x^3-2x^2-12x+9=0$ which has two pairs of equal roots.

16. Solve the equation $x^4+x^3-16x^2-4x+48=0$, given that the product of two of its roots is 6.

17. Solve the equation $6x^4-35x^3+62x^2-35x+6=0$, given that two roots are the reciprocals of the other two.

18. Solve the equation $x^4+2x^3-21x^2-22x+40=0$, given that the sum of two of its roots is equal to the sum of the other two.

19. Solve the equation $x^4+3x^3-4x^2-9x+9=0$, given that the product of two of its roots is equal to the product of the other two.

20. Solve the equation $x^4+2x^3-18x^2+6x+9=0$, given that the ratio of two of its roots is equal to the ratio of the other two.

21. Solve the equation $x^4-6x^3+18x^2-30x+25=0$ whose roots are of the form $(\alpha+i\beta)$ and $(\beta+i\alpha)$, where α and β are real.

22. If the equation $x^3-px^2+qx-r=0$ has a root of the form $(\alpha+i\alpha)$, where α is real, then show that

$$(p^2-2q)(q^2-2pr)=r^2. \qquad [C.\ H.\ 1989]$$

Hence or otherwise solve the equation $x^3-7x^2+20x-24=0$.

[C. H. 1978]

23. If the equation $x^4-px^3+qx^2-rx+s=0$ has two roots of the form $(\alpha+i\alpha)$, $(\beta+i\beta)$, where α and β are real, then show that

$$p^2=2q \quad \text{and} \quad r^2=2qs.$$

Hence or otherwise solve the equation

$$x^4+4x^3+8x^2-120x+900=0.$$

24. Solve the equations

(*i*) $x^3-x^2+3x-27=0$,

(*ii*) $x^4-2x^3+18x^2-18x+81=0$,

having distinct roots of equal moduli.

25. (*a*) Solve the equation $x^5-4x^4-10x^3+40x^2+9x-36=0$, having roots of the form $\pm a, \pm b, c$.

(*b*) Solve the equation $x^5-5x^4-5x^3+25x^2+4x-20=0$, having roots of the form $a, -a, b, -b, c$.

(*c*) Solve the equation $x^6-4x^5-11x^4+40x^3+11x^2-4x-1=0$, if it be given that $(\sqrt{2}+\sqrt{3})$ is its one root. [N. B. H. 2001]

26. Find the condition that the equation $x^4+px^3+qx^2+rx+s=0$ should have its roots $\alpha, \beta, \gamma, \delta$ connected by the relation

(*i*) $\alpha\beta=\gamma\delta$. (*ii*) $\beta+\gamma=\alpha+\delta$. [*N. B. H. 1981*]

(*iii*) $\alpha\beta+1=0$. (*iv*) $\alpha+\beta=0$. [*C. H. 1963*]

(*v*) $\alpha\beta=1$. (*vi*) $\alpha\beta+\gamma\delta=0$.

27. (*a*) If $\alpha, \beta, \gamma, \delta$ be the roots of $x^4-ax^3+bx^2-cx-1=0$, find the condition that $\alpha\beta-\gamma\delta=2$. [*C. H. 2003*]

(*b*) Let A, B, C be three points on the x-axis. The distances of A, B, C from the origin O are the roots of the equation $x^3+3px^2+3qx+r=0$. Find the condition that the point B bisects the segment AC. [*K. H. 2001*]

28. Show that the condition that the sum of two roots of the equation $x^4+mx^2+nx+p=0$ is equal to the product of the other two roots is $(2p-n)^2=(p-n)(p+m-n)^2$. [*C. H. 1972*]

29. Find the conditions that the roots of the equation

$$ax^4+4bx^3+6cx^2+4dx+e=0$$

are (*i*) equal in pairs, (*ii*) all equal.

30. (*a*) If α be a multiple root of order 3 of the equation $x^4+bx^2+cx+d=0$, then show that $\alpha=-\frac{8d}{3c}$. [*C. H. 1969*]

(*b*) If the equation $x^4+px^2+qx+r=0$ has three equal roots, then show that $8p^3+27q^2=0$ and $p^2+12r=0$. [*K. H. 2007*]

31. If the equation $x^5-10a^3x^2+b^4x+c^5=0$ has three equal roots, then show that $ab^4-9a^5+c^5=0$.

32. Show that all the roots of the equation

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots\ldots+p_{n-1}x+p_n=0$$

can be obtained when they are in A.P. [*B. H. 1969, 1992*]

Answers

1. (*i*) $-1, 2, 5$. (*ii*) $1, 3, 5$. (*iii*) $-5, -2, 1, 4$.

2. (*i*) $\frac{1}{2}, 2, 8$. (*ii*) $-\frac{2}{9}, \frac{2}{3}, -2$. (*iii*) $\frac{2}{3}, 2, 6$. (*iv*) $\frac{1}{3}, 1, 3, 9$.

3. (*a*) $\pm 2, 5$. (*b*) (*i*) $4, -4, 5$. (*ii*) $1, \frac{3}{2}, -\frac{3}{2}, -4$.

4. (*i*) $3, 6, -2$. (*ii*) $-\frac{3}{4}, -\frac{3}{2}, \frac{1}{3}$.

5. $-\frac{3}{2}, -2, 4$. **6.** (*a*) $3, -2, -\frac{3}{4}$. (*b*) $-2, 3, 6$. (*c*) $\frac{1}{2}, \frac{3}{2}, 4$.

7. (*a*) $\frac{1}{2}, -2, 1$. (*b*) $r^2+pr+q+1=0$. 8. (*b*) $r=5; 4, \frac{1}{2}(1\pm i\sqrt{3})$.

9. (*i*) $p(9q-2p^2)=27r$.

(*ii*) $a^3-4ab+8c=0, (a^2+4b)(11a^2-36b)+1600d=0$.

10. $p^2s=r^2$. 11. (*c*) $4, 2, \frac{4}{3}$.

14. (*a*) $1, 2, 1\pm i\sqrt{2}$. (*b*) $1, 2, 1\pm i\sqrt{2}$. 15. $1, 1, -3, -3$.

16. $\pm 2, 3, -4$. 17. $2, 3, \frac{1}{2}, \frac{1}{3}$.

18. $1, -2, 4, -5$. 19. $1, -3, \frac{1}{2}(-1\pm\sqrt{13})$.

20. $1, 3, -3\pm\sqrt{6}$. 21. $2\pm i, 1\pm 2i$. 22. $3, 2\pm 2i$.

23. $3\pm 3i, -5\pm 5i$.

24. (*i*) $3, -1\pm 2\sqrt{2}\,i$. (*ii*) $\pm 3i, 1\pm 2\sqrt{2}\,i$.

25. (*a*) $\pm 3, \pm 1, 4$. (*b*) $\pm 2, \pm 1, 5$. (*c*) $\sqrt{2}\pm\sqrt{3}, -\sqrt{2}\pm\sqrt{3}, 2\pm\sqrt{5}$.

26. (*i*) $r^2=p^2s$. (*ii*) $p^3=4pq-8r$.

(*iii*) $(r+p)(ps+r)+(s-1)^2(q+s+1)=0$. (*iv*) $r^2+p^2s=pqr$.

(*v*) $(ps-r)(p-r)+(s-1)^2(q-s-1)=0$. (*vi*) $p^2s+r^2=4qs$.

27. (*a*) $a^2=c^2+4b$. (*b*) $3pq=2p^3+r$.

29. (*i*) $ad^2=eb^2, 2b^3+a^2d=3abc$. (*ii*) $b^4=ab^2c=a^2bd=a^3e$.

3.3. Symmetric functions of the roots.

A function is said to be *symmetric* with respect to the roots if it remains unaltered in value when any two of the roots are interchanged. In a symmetric function of the roots, the sum of the exponents of the roots of each and every term is the same. This sum is called the *weight* of the symmetric function. The highest exponent is called its *order*. Thus in the symmetric function $\Sigma\alpha^3\beta^2$, the weight is $3+2=5$ and its order is 3.

Any symmetric function of the roots of an equation can be expressed in terms of the fundamental relations between the roots and the coefficients and hence in terms of the coefficients of the equation.

If $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the roots of the equation

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots\ldots+p_{n-1}x+p_n=0,$$

then $\Sigma\alpha_1=-p_1$,

$\Sigma\alpha_1\alpha_2=p_2$,

$\Sigma\alpha_1^2=(\Sigma\alpha_1)^2-2\Sigma\alpha_1\alpha_2=p_1^2-2p_2$,

$\Sigma\alpha_1^2\alpha_2=\Sigma\alpha_1\alpha_2.\Sigma\alpha_1-3\Sigma\alpha_1\alpha_2\alpha_3=3p_3-p_1p_2$,

$\Sigma\alpha_1^3=\Sigma\alpha_1^2.\Sigma\alpha_1-\Sigma\alpha_1^2\alpha_2=3p_1p_2-p_1^3-3p_3$, and so on.

3.4. Sums of powers of roots of an equation.

If $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the roots of an equation $f(x)=0$ of degree n, then $f(x)=a_0(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\ldots\ldots(x-\alpha_n)$, where a_0 is the coefficient of x^n in $f(x)$.

Taking logarithmic differentiation, we get

$$\frac{f'(x)}{f(x)}=\frac{1}{x-\alpha_1}+\frac{1}{x-\alpha_2}+\frac{1}{x-\alpha_3}+\ldots\ldots+\frac{1}{x-\alpha_n}$$

$$=x^{-1}(1-\alpha_1 x^{-1})^{-1}+x^{-1}(1-\alpha_2 x^{-1})^{-1}+\ldots\ldots$$

Now $x^{-1}(1-ax^{-1})^{-1}=x^{-1}+ax^{-2}+a^2x^{-3}+\ldots\ldots+a^n x^{-n-1}+\ldots\ldots$

Thus $\frac{f'(x)}{f(x)}=nx^{-1}+x^{-2}\Sigma\alpha_1+x^{-3}\Sigma\alpha_1{}^2+\ldots\ldots+x^{-n-1}\Sigma\alpha_1{}^n+\ldots\ldots$

Therefore the sum of the n-th powers of the roots, that is, $\Sigma\alpha_1{}^n$ is the coefficient of x^{-n-1} in the expansion of $\frac{f'(x)}{f(x)}$ in powers of x^{-1}.

3.5. Newton's theorem.

If $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the roots of the equation

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots\ldots+p_n=0$$

and if S_r denotes the sum of the r-th powers of the roots of the equation, r being a positive integer, then

$$S_r+p_1S_{r-1}+p_2S_{r-2}+\ldots\ldots+p_{r-1}S_1+rp_r=0, \text{ for } 1\le r<n$$

and $$S_r+p_1S_{r-1}+p_2S_{r-2}+\ldots\ldots+p_nS_{r-n}=0, \quad \text{for } r\ge n.$$

Let $f(x)=x^n+p_1x^{n-1}+p_2x^{n-2}+\ldots\ldots+p_n=(x-\alpha_1)(x-\alpha_2)\ldots\ldots(x-\alpha_n)$, since $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ are the roots of the equation $f(x)=0$.

Then $f'(x)=(x-\alpha_2)(x-\alpha_3)\ldots\ldots(x-\alpha_n)+(x-\alpha_1)(x-\alpha_3)\ldots\ldots(x-\alpha_n)+$

$$\ldots\ldots+(x-\alpha_1)(x-\alpha_2)\ldots\ldots(x-\alpha_{n-1})$$

$$=\frac{f(x)}{x-\alpha_1}+\frac{f(x)}{x-\alpha_2}+\ldots\ldots+\frac{f(x)}{x-\alpha_n}$$

$$=x^{n-1}+(\alpha_1+p_1)x^{n-2}+(\alpha_1{}^2+p_1\alpha_1+p_2)x^{n-3}$$

$$+\ldots\ldots+(\alpha_1{}^{n-1}+p_1\alpha_1{}^{n-2}+\ldots\ldots+p_{n-1})$$

$$+x^{n-1}+(\alpha_2+p_1)x^{n-2}+(\alpha_2{}^2+p_1\alpha_2+p_2)x^{n-3}$$

$$+\ldots\ldots+(\alpha_2{}^{n-1}+p_1\alpha_2{}^{n-2}+\ldots\ldots+p_{n-1})$$

$$+ \cdots\cdots + x^{n-1} + (\alpha_n + p_1)\, x^{n-2} + (\alpha_n^{\,2} + p_1\alpha_n + p_2)\, x^{n-3}$$
$$+ \cdots\cdots + (\alpha_n^{\,n-1} + p_1\, \alpha_n^{\,n-2} + \cdots\cdots + p_{n-1})$$
$$= nx^{n-1} + (S_1 + np_1)\, x^{n-2} + (S_2 + p_1 S_1 + np_2)\, x^{n-3}$$
$$+ \cdots\cdots + (S_{n-1} + p_1\, S_{n-2} + \cdots\cdots + n\, p_{n-1}) .$$

Also $f'(x) = nx^{n-1} + (n-1)\, p_1 x^{n-2} + (n-2)\, p_2\, x^{n-3} + \cdots\cdots + p_{n-1}$.

Comparing these, we get

$$S_1 + np_1 = (n-1)\, p_1 ,$$
$$S_2 + p_1\, S_1 + np_2 = (n-2)\, p_2 ,$$
$$\cdots \quad \cdots \quad \cdots$$
$$\cdots \quad \cdots \quad \cdots$$
$$S_{n-1} + p_1\, S_{n-2} + \cdots\cdots + np_{n-1} = p_{n-1} .$$

Therefore
$$S_1 + p_1 = 0,$$
$$S_2 + p_1\, S_1 + 2p_2 = 0 ,$$
$$\cdots \quad \cdots \quad \cdots$$
$$\cdots \quad \cdots \quad \cdots$$
$$S_{n-1} + p_1\, S_{n-2} + \cdots\cdots + (n-1)\, p_{n-1} = 0.$$

Combining them, we get the result for $1 \le r < n$.

When $r = n$, putting $x = \alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ successively in the given equation and adding them, we get

$$S_n + p_1\, S_{n-1} + p_2\, S_{n-2} + \cdots\cdots + n\, p_n = 0. \qquad \ldots \quad (1)$$

When $r > n$, multiplying the given equation by x^{r-n}, we get an equation of degree r, namely $x^r + p_1\, x^{r-1} + p_2\, x^{r-2} + \cdots\cdots + p_n\, x^{r-n} = 0$, whose roots are $\alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ and a multiple root 0 of multiplicity $(r-n)$.

Putting $x = \alpha_1, \alpha_2, \ldots\ldots, \alpha_n$ successively in this equation and adding them, we get

$$S_r + p_1\, S_{r-1} + p_2\, S_{r-2} + \cdots\cdots + p_n\, S_{r-n} = 0 . \qquad \ldots \quad (2)$$

Combining (1) and (2), we get the result for $r \ge n$.

3.6. Illustrative Examples.

Ex. 1. *If a, b, c be the roots of the equation $x^3 - px^2 + qx - r = 0$, then find the value of* (*i*) $\Sigma\left(\frac{b}{c} + \frac{c}{b}\right)$. (*ii*) $\Sigma a^2 b^2$.

Since a, b, c are the roots of the given equation, we have

$$a + b + c = p , \quad ab + bc + ca = q , \quad abc = r .$$

(i) $\Sigma\left(\frac{b}{c}+\frac{c}{b}\right)=\Sigma\frac{b^2+c^2}{bc}=\frac{b^2+c^2}{bc}+\frac{c^2+a^2}{ca}+\frac{a^2+b^2}{ab}$

$$=\frac{1}{abc}(ab^2+ac^2+bc^2+ba^2+ca^2+cb^2)$$

$$=\frac{1}{abc}\{(a+b+c)(ab+bc+ca)-3abc\}=\frac{1}{r}(pq-3r),$$

(ii) $\Sigma a^2b^2=a^2b^2+b^2c^2+c^2a^2$

$$=(ab+bc+ca)^2-2abc(a+b+c)=q^2-2pr.$$

Ex. 2. *If α, β, γ be the roots of the equation $x^3+px^2+qx+r=0$, then find the value of*

(i) $\Sigma\alpha^3\beta^3$. (ii) $(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)$. (iii) $\Sigma(\alpha-\beta)^2$.

We have $\alpha+\beta+\gamma=-p$, $\alpha\beta+\beta\gamma+\gamma\alpha=q$, $\alpha\beta\gamma=-r$.

(i) We have the identity

$$(a+b+c)^3=a^3+b^3+c^3+3(b+c)(c+a)(a+b)$$

$$=a^3+b^3+c^3+3\{(a+b+c)(ab+bc+ca)-abc\}.$$

Hence $\alpha^3\beta^3+\beta^3\gamma^3+\gamma^3\alpha^3$

$$=(\alpha\beta+\beta\gamma+\gamma\alpha)^3-3\{\alpha\beta\gamma(\alpha+\beta+\gamma)(\alpha\beta+\beta\gamma+\gamma\alpha)-\alpha^2\beta^2\gamma^2\}$$

$$=q^3-3\{(-r)(-p)q-r^2\}=q^3-3pqr+3r^2.$$

(ii) $(\alpha+\beta)(\beta+\gamma)(\gamma+\alpha)$

$$=(\alpha+\beta+\gamma-\gamma)(\alpha+\beta+\gamma-\alpha)(\alpha+\beta+\gamma-\beta)$$

$$=(-p-\gamma)(-p-\alpha)(-p-\beta)=-(p+\alpha)(p+\beta)(p+\gamma)$$

$$=-p^3-p^2(\alpha+\beta+\gamma)-p(\alpha\beta+\beta\gamma+\gamma\alpha)-\alpha\beta\gamma$$

$$=-p^3+p^3-pq+r=r-pq.$$

(iii) $\Sigma(\alpha-\beta)^2=(\alpha-\beta)^2+(\beta-\gamma)^2+(\gamma-\alpha)^2$

$$=(\alpha^2-2\alpha\beta+\beta^2)+(\beta^2-2\beta\gamma+\gamma^2)+(\gamma^2-2\gamma\alpha+\alpha^2)$$

$$=2(\alpha^2+\beta^2+\gamma^2)-2(\alpha\beta+\beta\gamma+\gamma\alpha)$$

$$=2(p^2-2q)-2q=2(p^2-3q).$$

Ex. 3. *If $\alpha, \beta, \gamma, \delta$ be the roots of the biquadratic equation $x^4+px^3+qx^2+rx+s=0$, then calculate the value of*

(i) $\Sigma\alpha^3$. (ii) $\Sigma\alpha^3\beta$. (iii) $\Sigma\alpha^4$. [*B. H. 1994*]

Here $\alpha+\beta+\gamma+\delta=-p$,

$\alpha\beta+\alpha\gamma+\alpha\delta+\beta\gamma+\beta\delta+\gamma\delta=q$,

$\alpha\beta\gamma+\alpha\beta\delta+\beta\gamma\delta+\alpha\gamma\delta=-r$

and $\alpha\beta\gamma\delta=s$.

(i) We have $(\Sigma\alpha^2)(\Sigma\alpha)=\Sigma\alpha^3+\Sigma\alpha^2\beta$.

Therefore $\Sigma\alpha^3 = (\Sigma\alpha^2)(\Sigma\alpha) - \Sigma\alpha^2\beta$

$= \{(\Sigma\alpha)^2 - 2\Sigma\alpha\beta\}\Sigma\alpha - \{(\Sigma\alpha)(\Sigma\alpha\beta) - 3\Sigma\alpha\beta\gamma\}$

$= \{(-p)^2 - 2q\}(-p) - \{(-p)q - 3(-r)\}$

$= (p^2 - 2q)(-p) - (-pq + 3r)$

$= 3pq - p^3 - 3r.$

(ii) We have $(\Sigma\alpha\beta\gamma)(\Sigma\alpha) = \Sigma\alpha^2\beta\gamma + 4\alpha\beta\gamma\delta.$

Therefore $\Sigma\alpha^2\beta\gamma = (\Sigma\alpha\beta\gamma)(\Sigma\alpha) - 4\alpha\beta\gamma\delta = pr - 4s.$

Now $\Sigma\alpha^3\beta = \Sigma\alpha^2\Sigma\alpha\beta - \Sigma\alpha^2\beta\gamma$

$= \{(\Sigma\alpha)^2 - 2\Sigma\alpha\beta\}\Sigma\alpha\beta - \Sigma\alpha^2\beta\gamma$

$= (p^2 - 2q)q - (pr - 4s).$

(iii) We have $\Sigma\alpha^4 = \Sigma(\alpha^2)^2 = (\Sigma\alpha^2)^2 - 2\Sigma\alpha^2\beta^2$

$= \{(\Sigma\alpha)^2 - 2\Sigma\alpha\beta\}^2 - 2\{(\Sigma\alpha\beta)^2 - 2\Sigma\alpha^2\beta\gamma - 6\alpha\beta\gamma\delta\}$

$= (p^2 - 2q)^2 - 2\{q^2 - 2(pr - 4s) - 6s\}$

$= (p^2 - 2q)^2 - 2(q^2 - 2pr + 2s)$

$= p^4 - 4p^2q + 4pr + 2q^2 - 4s.$

Second method :

Using the method of Article 3. 4, we have here

$$f(x) = x^4 + px^3 + qx^2 + rx + s$$

and $$f'(x) = 4x^3 + 3px^2 + 2qx + r.$$

Now $\Sigma\alpha^4$ is the coefficient of x^{-5} in

$$\frac{f'(x)}{f(x)} = \frac{4x^3 + 3px^2 + 2qx + r}{x^4 + px^3 + qx^2 + rx + s}.$$

By simple division, we get the coefficient of x^{-5} in $\dfrac{f'(x)}{f(x)}$ as

$$p^4 - 4p^2q + 4pr + 2q^2 - 4s.$$

Hence $\Sigma\alpha^4 = p^4 - 4p^2q + 4pr + 2q^2 - 4s.$

Ex. 4. *If* α, β, γ *be the roots of the equation* $x^3 + px + q = 0$, *then find the value of*

(i) $\Sigma\dfrac{1}{\alpha + \beta}.$

(ii) $(\beta + \gamma - 2\alpha)(\gamma + \alpha - 2\beta)(\alpha + \beta - 2\gamma).$ *(iii)* $\Sigma\alpha^5.$

We have here $\alpha + \beta + \gamma = 0$, $\alpha\beta + \beta\gamma + \gamma\alpha = p$, $\alpha\beta\gamma = -q.$

(*i*) $\Sigma\frac{1}{\alpha+\beta}=\frac{1}{\alpha+\beta}+\frac{1}{\beta+\gamma}+\frac{1}{\gamma+\alpha}=\frac{1}{-\gamma}+\frac{1}{-\alpha}+\frac{1}{-\beta}$

$$=-\left(\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}\right)=-\frac{\alpha\beta+\beta\gamma+\gamma\alpha}{\alpha\beta\gamma}=\frac{p}{q}.$$

(*ii*) $\beta+\gamma-2\alpha=\alpha+\beta+\gamma-3\alpha=-3\alpha$.

Similarly, $\gamma+\alpha-2\beta=-3\beta$ and $\alpha+\beta-2\gamma=-3\gamma$.

Thus $(\beta+\gamma-2\alpha)(\gamma+\alpha-2\beta)(\alpha+\beta-2\gamma)$

$$=(-3\alpha)(-3\beta)(-3\gamma)=-27\,\alpha\beta\gamma=27q.$$

(*iii*) $\Sigma\alpha^5=\Sigma\alpha^3\Sigma\alpha^2-\Sigma\alpha^3\beta^2$

$$=\{(\Sigma\alpha)^3-3(\beta+\gamma)(\gamma+\alpha)(\alpha+\beta)\}\{(\Sigma\alpha)^2-2\Sigma\alpha\beta\}$$
$$-(\Sigma\alpha\Sigma\alpha^2\beta^2-\Sigma\alpha^2\beta^2\gamma)$$
$$=-3(-\alpha)(-\beta)(-\gamma)(-2p)-(-\alpha\beta\gamma\Sigma\alpha\beta)$$
$$=6pq-pq=5pq.$$

Ex. 5. *If* α,β,γ *be the roots of the equation* $x^3+px^2+qx+r=0$, *then find the equation whose roots are*

(*i*) $\beta\gamma,\gamma\alpha,\alpha\beta$. (*ii*) $\alpha^2,\beta^2,\gamma^2$. (*iii*) $\beta+\gamma,\gamma+\alpha,\alpha+\beta$.

We have here $\alpha+\beta+\gamma=-p$, $\alpha\beta+\beta\gamma+\gamma\alpha=q$, $\alpha\beta\gamma=-r$.

(*i*) $S_1=\beta\gamma+\gamma\alpha+\alpha\beta=q$,

$$S_2=\alpha^2\beta\gamma+\beta^2\gamma\alpha+\gamma^2\alpha\beta=\alpha\beta\gamma(\alpha+\beta+\gamma)=rp,$$
$$S_3=\alpha^2\beta^2\gamma^2=r^2.$$

The required equation is $y^3-S_1y^2+S_2y-S_3=0$

or, $y^3-qy^2+rpy-r^2=0$.

(*ii*) $S_1=\alpha^2+\beta^2+\gamma^2=(\alpha+\beta+\gamma)^2-2(\alpha\beta+\beta\gamma+\gamma\alpha)=p^2-2q$,

$$S_2=\alpha^2\beta^2+\beta^2\gamma^2+\gamma^2\alpha^2=(\Sigma\alpha\beta)^2-2\alpha\beta\gamma(\Sigma\alpha)=q^2-2rp,$$
$$S_3=\alpha^2\beta^2\gamma^2=r^2.$$

Hence the required equation is

$$y^3-S_1y^2+S_2y-S_3=0$$

or, $y^3-(p^2-2q)y^2+(q^2-2rp)y-r^2=0$.

(*iii*) Here $S_1=2(\alpha+\beta+\gamma)=-2p$,

$$S_2=(\alpha+\beta+\gamma)^2+(\alpha\beta+\beta\gamma+\gamma\alpha)=p^2+q,$$
$$S_3=(-p-\alpha)(-p-\beta)(-p-\gamma)$$
$$=-p^3-p^2(-p)-pq+r$$
$$=r-pq.$$

Hence the required equation is

$$y^3 - S_1 y^2 + S_2 y - S_3 = 0$$

or, $$y^3 + 2py^2 + (p^2 + q)y + (pq - r) = 0.$$

Examples III (B)

1. If α, β, γ be the roots of the equation

$$x^3 + px^2 + qx + r = 0,$$

then find, in terms of p, q, r, the value of

(*i*) $\alpha^2 + \beta^2 + \gamma^2$. (*ii*) $\beta^2\gamma^2 + \gamma^2\alpha^2 + \alpha^2\beta^2$. (*iii*) $\Sigma\alpha^4$.

(*iv*) $(\beta + \gamma - 3\alpha)(\gamma + \alpha - 3\beta)(\alpha + \beta - 3\gamma)$.

(*v*) $\dfrac{1}{\alpha^2} + \dfrac{1}{\beta^2} + \dfrac{1}{\gamma^2}$. (*vi*) $\dfrac{1}{\alpha^3} + \dfrac{1}{\beta^3} + \dfrac{1}{\gamma^3}$.

(*vii*) $\dfrac{\alpha}{\beta} + \dfrac{\alpha}{\gamma} + \dfrac{\beta}{\alpha} + \dfrac{\beta}{\gamma} + \dfrac{\gamma}{\alpha} + \dfrac{\gamma}{\beta}$. (*viii*) $\Sigma\dfrac{1}{\alpha^2\beta}$. [*N. B. H.1987*]

(*ix*) $(\beta + \gamma - \alpha)^3 + (\gamma + \alpha - \beta)^3 + (\alpha + \beta - \gamma)^3$. [*B. H.1990*]

2. If α, β, γ be the roots of the equation $x^3 - px^2 + qx - r = 0$, then find, in terms of p, q, r, the value of

(*i*) $\dfrac{1}{\alpha} + \dfrac{1}{\beta} + \dfrac{1}{\gamma}$. (*ii*) $\dfrac{1}{\beta^2\gamma^2} + \dfrac{1}{\gamma^2\alpha^2} + \dfrac{1}{\alpha^2\beta^2}$.

(*iii*) $\Sigma\dfrac{\beta^2 + \gamma^2}{\beta + \gamma}$. (*iv*) $\Sigma\dfrac{\alpha\beta + \gamma^2}{\alpha + \beta}$. (*v*) $\Sigma\left(\dfrac{\alpha - \beta}{\alpha + \beta}\right)^2$.

(*vi*) $\Sigma(\alpha - \beta)^4$. (*vii*) $\Sigma\alpha^6$. (*viii*) $\Sigma(\beta^3 - \gamma^3)^2$.

3. If α, β, γ be the roots of the equation $x^3 + qx + r = 0$, then find, in terms of q and r, the value of

(*i*) $(\beta - \gamma)^2 + (\gamma - \alpha)^2 + (\alpha - \beta)^2$.

(*ii*) $(\beta + \gamma)^{-1} + (\gamma + \alpha)^{-1} + (\alpha + \beta)^{-1}$.

(*iii*) $(\beta + \gamma - \alpha)^{-1} + (\gamma + \alpha - \beta)^{-1} + (\alpha + \beta - \gamma)^{-1}$.

(*iv*) $\Sigma\dfrac{\alpha^2}{\beta\gamma}$. (*v*) $\Sigma\alpha^3\beta$.

4. Find the sum of the squares of the reciprocals of the roots of the equation $x^3 - 2x + 1 = 0$.

5. If α, β, γ be the roots of the equation $x^3 + x + 1 = 0$, then prove that $(\alpha^2 + 1)(\beta^2 + 1)(\gamma^2 + 1) = 1$.

6. If α, β, γ be the roots of the equation

$$px^3 + 3qx^2 + 3rx + s = 0,$$

then find, in terms of p, q, r, s, the value of

(*i*) $\Sigma \alpha^2$. (*ii*) $\Sigma \alpha^3$. (*iii*) $\Sigma \alpha^2 \beta$.

(*iv*) $\Sigma \frac{1}{\beta + \gamma}$. (*v*) $\Sigma (\beta - \gamma)^2$. (*vi*) $(\beta + \gamma)(\gamma + \alpha)(\alpha + \beta)$.

(*vii*) $\Sigma \alpha^2 \beta^2 \gamma$. (*viii*) $\Sigma (\alpha - \beta)^2 \gamma$. (*ix*) $\Sigma (\alpha - \beta)^2 \gamma^2$.

7. If α, β, γ be the roots of the cubic $ax^3 + 3bx^2 + 3cx + d = 0$, then find the value of the expression $(a\alpha + b)(a\beta + b)(a\gamma + b)$ in terms of the coefficients a, b, c, d. [*C. H. 1969*]

8. If a, b, c be the roots of the equation $x^3 + qx + r = 0$, then show that

(*i*) $a^3 + b^3 + c^3 = -3r$.

(*ii*) $a^4 + b^4 + c^4 = 2(ab + bc + ca)^2$.

(*iii*) $a^5 + b^5 + c^5 + 5abc(bc + ca + ab) = 0$.

[*C. H. 1975 ; N. B. H. 1988*],

(*iv*) $6s_5 = 5s_2 s_3$, where $s_n = a^n + b^n + c^n$. [*C. H.1970*]

(*v*) $\Sigma \frac{1}{a^2 - bc} = -\frac{3}{q}$. (*vi*) $\Sigma \frac{2bc - a^2}{b + c - a} = \frac{q^2}{r}$.

9. Show that the sum of the fourth powers of the roots of the equation $x^3 - 2x^2 + x - 1 = 0$ is 10.

10. Show that the sum of the sixth powers of the roots of the equation $x^3 - x = 1$ is 5.

11. Find the sums of (*i*) the squares, (*ii*) the cubes, (*iii*) the fourth powers of the roots of the equation $x^4 + qx^2 + rx + s = 0$.

If $\alpha, \beta, \gamma, \delta$ be the roots of this equation, then show that

$$\frac{s_5}{5} = \frac{s_2}{2} \cdot \frac{s_3}{3}, \text{ where } s_n = \Sigma \alpha^n.$$

12. If $\alpha, \beta, \gamma, \delta$ be the roots of the equation $x^4 - 4x + 3 = 0$, then find the values of $\Sigma \alpha^4$ and $\Sigma \frac{1}{\alpha^2 \beta \gamma}$.

13. If $\alpha, \beta, \gamma, \delta$ be the roots of the equation $x^4 + px^3 + qx^2 + rx + s = 0$, then find, in terms of p, q, r, s, the value of

(*i*) $\Sigma \alpha^2 \beta$. [*B. H.1989*] (*ii*) $\Sigma \alpha^2 \beta\gamma$.

(*iii*) $\Sigma \alpha^3 \beta\gamma$. (*iv*) $\Sigma \alpha^2 \beta^2 \gamma^2$. [*C. H.1987*]

(*v*) $\Sigma \frac{\alpha\beta}{\gamma}$. [*B. H. 2000*] (*vi*) $\Sigma \frac{\alpha\beta}{\gamma^2}$. [*N. B. H. 1985*]

(*vii*) $\Sigma (\alpha - \beta)^2 \gamma\delta$. (*viii*) $\Sigma \alpha \beta^2 \gamma^2$. [*V. H. 1997*]

(*ix*) $(\alpha^2+1)(\beta^2+1)(\gamma^2+1)(\delta^2+1)$.

(*x*) $(\beta\gamma + \alpha\delta)(\gamma\alpha + \beta\delta)(\alpha\beta + \gamma\delta)$.

14. If $\alpha, \beta, \gamma, \delta$ be the roots of the biquadratic

$$x^4 - px^3 + qx^2 - rx + s = 0,$$

then find, in terms of p, q, r, s, the value of

(*i*) $\Sigma \frac{\alpha+\beta}{\alpha\beta}$. (*ii*) $\Sigma \frac{1}{\alpha\beta}$. (*iii*) $\Sigma \frac{1}{\alpha^2}$. (*iv*) $\Sigma \frac{\alpha}{\beta}$.

(*v*) $\Sigma \frac{\alpha^2}{\beta}$. (*vi*) $\Sigma (\alpha - \beta)^2$. (*vii*) $\Sigma \alpha^2 \beta^2$. (*viii*) $\Sigma \frac{1}{\alpha^2 \beta}$.

(*ix*) $\Sigma (\alpha - \beta)(\alpha - \gamma)(\alpha - \delta)$.

(*x*) $(\beta\gamma - \alpha\delta)(\gamma\alpha - \beta\delta)(\alpha\beta - \gamma\delta)$.

(*xi*) $(\beta + \gamma - \alpha - \delta)(\gamma + \alpha - \beta - \delta)(\alpha + \beta - \gamma - \delta)$.

(*xii*) $(\beta - \gamma)^2 (\alpha - \delta)^2 + (\gamma - \alpha)^2 (\beta - \delta)^2 + (\alpha - \beta)^2 (\gamma - \delta)^2$.

15. If $\alpha, \beta, \gamma, \delta$ be the roots of the biquadratic

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0,$$

then prove that $a^2 \Sigma \alpha^2 \beta = 12 (ad - 2bc)$,

$$a^2 \Sigma (\alpha - \beta)^2 \gamma^2 \delta^2 = 48 (d^2 - ce) \quad [V. H. 1989]$$

and $$a^3 \Sigma \alpha\beta (\gamma + \delta)^3 = 16 (3acd - 2abe - 4b^2 d).$$

16. Show that the sum of the fifth powers of the roots of the equation $x^4 - 3x^3 + 5x^2 - 12x + 4 = 0$ is 123.

17. If $\alpha, \beta, \gamma, \delta$ be the roots of the equation

$$x^4 + p_2 x^2 + p_3 x + p_4 = 0,$$

then show that $\Sigma \alpha^6 = 6p_2 p_4 + 3p_3{}^2 - 2p_2{}^3$ and $\Sigma \alpha^7 = -7p_3 (p_2{}^2 - p_4)$.

18. (*a*) Show that the sum of the fourth powers of the roots of the equation $x^5 + px^3 + px^2 + s = 0$ is $2p^2$.

(*b*) Show that the sum of the sixth powers of the roots of the equation $x^5 + ax^4 + bx^2 + c = 0$ is $(a^6 + 6a^3 b + 3b^2 + 6ac)$. [*C. H. 1979*]

19. Find the area of the triangle of which the lengths of the sides are the roots of the equation $x^3 - ax^2 + bx - c = 0$. [K. H. 2002]

20. If $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the roots of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots\ldots + p_{n-1} x + p_n = 0, p_n \neq 0,$$

then find the value of

(*i*) $\Sigma \alpha_1^2$. (*ii*) $\Sigma \frac{1}{\alpha_1}$. (*iii*) $\Sigma \frac{\alpha_1^2 + \alpha_2^2}{\alpha_1 \alpha_2}$. (*iv*) $\Sigma \frac{\alpha_1}{\alpha_2^2}$.

(*v*) $\Sigma \alpha_1^2 \alpha_2 \alpha_3$. (*vi*) $\Sigma \alpha_1^3$. [B. H. 1985]

(*vii*) $\Sigma (\alpha_1 - \alpha_2)^2 \alpha_3 \alpha_4 \ldots\ldots \alpha_n$. (*viii*) $\Sigma \frac{\alpha_1^3}{\alpha_2^2}$.

21. If α, β, γ be the roots of the equation $x^3 + qx + r = 0$, then form the equation whose roots are

(*i*) $\beta^2\gamma^2, \gamma^2\alpha^2, \alpha^2\beta^2$. (*ii*) $\frac{\beta+\gamma}{\alpha^2}, \frac{\gamma+\alpha}{\beta^2}, \frac{\alpha+\beta}{\gamma^2}$.

(*iii*) $\alpha(\beta+\gamma), \beta(\gamma+\alpha), \gamma(\alpha+\beta)$.

(*iv*) $\frac{\beta}{\gamma}+\frac{\gamma}{\beta}, \frac{\gamma}{\alpha}+\frac{\alpha}{\gamma}, \frac{\alpha}{\beta}+\frac{\beta}{\alpha}$. (*v*) $\frac{\beta\gamma}{\alpha}, \frac{\gamma\alpha}{\beta}, \frac{\alpha\beta}{\gamma}$.

(*vi*) $(\beta+\gamma-2\alpha), (\gamma+\alpha-2\beta), (\alpha+\beta-2\gamma)$.

22. (*a*) If α, β, γ be the roots of the cubic $x^3 + qx - r = 0$, then find the equation whose roots are $(\alpha^2+\beta\gamma)$, $(\beta^2+\gamma\alpha)$, $(\gamma^2+\alpha\beta)$.

Hence find the value of $\Sigma(\alpha^2+\beta\gamma)(\beta^2+\gamma\alpha)$.

(*b*) If $\alpha+\beta+\gamma=1$, $\alpha^2+\beta^2+\gamma^2=3$ and $\alpha^3+\beta^3+\gamma^3=7$, then show that the equation, whose roots are $(\alpha^2-\beta\gamma)$, $(\beta^2-\gamma\alpha)$ and $(\gamma^2-\alpha\beta)$, is $x^3-4x^2+4x-2=0$.

(*c*) If α, β, γ be the roots of the cubic $x^3 - 21x + 35 = 0$, then show that $(\alpha^2 + 2\alpha - 14)$ is equal to either β or γ. [V. H. 2008]

23. If $\alpha, \beta, \gamma, \delta$ be the roots of the biquadratic $x^4 + px^3 + qx^2 + rx + s = 0$, then find the equation whose roots are

$$(\beta\gamma+\alpha\delta), (\gamma\alpha+\beta\delta), (\alpha\beta+\gamma\delta).$$

Hence find the value of

$$(\alpha+\beta)(\alpha+\gamma)(\alpha+\delta)(\beta+\gamma)(\beta+\delta)(\gamma+\delta).$$

24. If α be a non-real root of $x^7 = 1$, then find the equation whose roots are $(\alpha+\alpha^6), (\alpha^2+\alpha^5), (\alpha^3+\alpha^4)$. [V. H. 2006; C. H. 2009]

25. Form the biquadratic whose roots are

$$(\alpha+2\alpha^4), (\alpha^2+2\alpha^3), (\alpha^3+2\alpha^2) \text{ and } (\alpha^4+2\alpha),$$

where α is an imaginary root of the equation $x^5 - 1 = 0$.

Answers

1. (*i*) p^2-2q. (*ii*) q^2-2pr. (*iii*) $p^4-4p^2q+2q^2+4pr$.

(*iv*) $3p^3-16pq+64r$. (*v*) $\frac{q^2-2pr}{r^2}$. (*vi*) $\frac{3pqr-q^3-3r^2}{r^3}$.

(*vii*) $\frac{pq-3r}{r}$. (*viii*) $\frac{3r-pq}{r^2}$. (*ix*) $24r-p^3$.

2. (*i*) $\frac{q}{r}$. (*ii*) $\frac{p^2-2q}{r^2}$. (*iii*) $\frac{2(p^2q-2pr-q^2)}{pq-r}$.

(*iv*) $\frac{p^4-3p^2q+5pr+q^2}{pq-r}$. (*v*) $\frac{3p^2q^2-4p^3r-4q^3-2pqr-9r^2}{(pq-r)^2}$.

(*vi*) $2(p^4-6p^2q+9q^2)$.

(*vii*) $(p^3-3pq+3r)^2-2(q^3-3pqr+3r^2)$.

(*viii*) $2(p^6-6p^4q+6p^3r+9p^2q^2-9pqr-3q^3)$.

3. (*i*) $-6q$. (*ii*) $\frac{q}{r}$. (*iii*) $\frac{q}{2r}$. (*iv*) 3. (*v*) $-2q^2$. **4.** 4.

6. (*i*) $\frac{3(3q^2-2pr)}{p^2}$. (*ii*) $\frac{3}{p^3}(9pqr-p^2s-9q^3)$. (*iii*) $\frac{3ps-9qr}{p^2}$.

(*iv*) $\frac{3pr+9q^2}{ps-9qr}$. (*v*) $\frac{18}{p^2}(q^2-pr)$. (*vi*) $\frac{1}{p^2}(ps-9qr)$.

(*vii*) $-\frac{3rs}{p^2}$. (*viii*) $\frac{9(ps-qr)}{p^2}$. (*ix*) $\frac{18(r^2-qs)}{p^2}$.

7. $3abc-a^2d-2b^3$.

11. (*i*) $-2q$. (*ii*) $-3r$. (*iii*) $2(q^2-2s)$. **12.** $-12, -\frac{4}{3}$.

13. (*i*) $3r-pq$. (*ii*) $pr-4s$. (*iii*) $ps-r(p^2-2q)$.

(*iv*) r^2-2qs. (*v*) $\frac{3ps-qr}{s}$. (*vi*) $\frac{qr^2-2q^2s-prs+4s^2}{s^2}$.

(*vii*) $pr-16s$. (*viii*) $3ps-qr$. (*ix*) $(1-q+s)^2+(p-r)^2$.

(*x*) r^2+p^2s-4qs.

14. (*i*) $\frac{3r}{s}$. (*ii*) $\frac{q}{s}$. (*iii*) $\frac{r^2-2qs}{s^2}$. (*iv*) $\frac{pr-4s}{s}$. (*v*) $\frac{p^2r-2qr-ps}{s}$.

(*vi*) $3p^2-8q$. (*vii*) $q^2-2pr+2s$. (*viii*) $\frac{qr-3ps}{s^2}$. (*ix*) $p^3-4pq+8r$.

(*x*) r^2-p^2s. (*xi*) $4pq-p^3-8r$. (*xii*) $2(q^2-3pr+12s)$.

19. $\frac{1}{4}\sqrt{a(4ab-a^3-8c)}$ square units.

20. (*i*) $p_1^2 - 2p_2$. (*ii*) $-\frac{p_{n-1}}{p_n}$. (*iii*) $\frac{p_1 p_{n-1}}{p_n} - n$.

(*iv*) $\frac{p_{n-1}p_n - p_1 p_{n-1}^2 + 2p_1 p_{n-1} p_n}{p_n^2}$. (*v*) $p_1 p_3 - 4p_4$.

(*vi*) $3p_1 p_2 - p_1^3 - 3p_3$. (*vii*) $(-1)^n (p_1 p_{n-1} - n^2 p_n)$.

(*viii*) $p_1 + \frac{(3p_1 p_2 - p_1^3 - 3p_3)(p_{n-1}^2 - 2p_n p_{n-2})}{p_n^2}$.

21. (*i*) $y^3 - q^2 y^2 - 2qr^2 y - r^4 = 0$. (*ii*) $ry^3 - qy^2 - 1 = 0$.

(*iii*) $y^3 - 2qy^2 + q^2 y + r^2 = 0$. (*iv*) $r^2 (y+1)^3 + q^3 (y+2) = 0$.

(*v*) $ry^3 + q^2 y^2 - 2qry + r^2 = 0$. (*vi*) $y^3 + 9qy - 27r = 0$.

22. (*a*) $y^3 + qy^2 - q^2 y - (q^3 + 8r^2) = 0$; $(-q^2)$.

23. $y^3 - qy^2 + (pr - 4s) y - (r^2 - 4qs + p^2 s) = 0$; $pqr - r^2 - p^2 s$.

24. $y^3 + y^2 - 2y - 1 = 0$. 25. $y^4 + 3y^3 - y^2 - 3y + 11 = 0$.

3.7. Transformation of equations.

A given equation can be transformed to an equation whose roots are related in some way to the given equation.

Let $f(x) = 0$ be a given equation . Let it be required to find a new equation in y, say, whose roots are connected with the roots of the given equation by a certain relation of the form $\phi(x, y) = 0$.

The transformed equation can be obtained by eliminating x between $f(x) = 0$ and $\phi(x, y) = 0$.

This will give the equation satisfied by y.

Let $\alpha_1, \alpha_2, \alpha_3, \ldots\ldots, \alpha_n$ be the roots of the equation

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots\ldots + p_{n-1} x + p_n = 0. \quad \ldots \quad (1)$$

(*i*) *Multiplication of the roots by a constant.*

We are to form an equation whose roots will be

$m\alpha_1, m\alpha_2, m\alpha_3, \ldots\ldots, m\alpha_n$, m being a constant.

Let us substitute $y = mx$, that is, $x = \frac{y}{m}$ in (1) and we get

$$\frac{y^n}{m^n} + p_1 \frac{y^{n-1}}{m^{n-1}} + p_2 \frac{y^{n-2}}{m^{n-2}} + \ldots\ldots + p_{n-1} \frac{y}{m} + p_n = 0$$

or, $y^n + mp_1 y^{n-1} + m^2 p_2 y^{n-2} + \ldots\ldots$

$$\ldots\ldots + m^{n-1} p_{n-1} y + m^n p_n = 0. \quad \ldots \quad (2)$$

The relation $y = mx$ suggests that the roots of (2) are each m times the roots of (1). Thus to multiply the roots of an equation by a constant m, we obtain the transformed equation by *multiplying the successive coefficients of the given equation beginning from the second by*

$$m, m^2, \ldots\ldots, m^n.$$

Cor. 1. To transform an equation into another whose roots are those of the proposed equation with contrary signs, m is (-1), that is, the transformation is effected by changing the signs of every alternate term of the given equation beginning with the second.

Cor. 2. To transform an equation into another whose roots are those of the proposed equation divided by certain constant m, the multiplication of the roots by $\frac{1}{m}$ is effected.

Note. If the equation be incomplete, the missing terms are to be supplied with zero coefficients and then the above transformations are to be effected.

(ii) Formation of an equation with the reciprocals of roots.

We are to form an equation whose roots are

$$\frac{1}{\alpha_1}, \frac{1}{\alpha_2}, \frac{1}{\alpha_3}, \ldots\ldots, \frac{1}{\alpha_n}.$$

Let us substitute $y = \frac{1}{x}$, that is, $x = \frac{1}{y}$ in (1) and we get

$$\frac{1}{y^n} + p_1 \frac{1}{y^{n-1}} + p_2 \frac{1}{y^{n-2}} + \ldots\ldots + p_{n-1} \frac{1}{y} + p_n = 0$$

or, $$p_n y^n + p_{n-1} y^{n-1} + \ldots\ldots + p_1 y + 1 = 0. \quad \ldots \quad (3)$$

The relation $y = \frac{1}{x}$ suggests that the roots of (3) are the reciprocals of the roots of (1). Thus to transform an equation into one whose roots are the reciprocals of the roots of the given equation, we are to *replace x by y^{-1} and then multiply by y^n.*

(iii) To increase or diminish the roots of the given equation.

We are to find an equation whose roots are

$$\alpha_1 - h, \alpha_2 - h, \ldots\ldots, \alpha_n - h, \ (h > 0)$$

that is, each root is diminished by h.

Let us substitute $y = x - h$, that is, $x = y + h$, where x and y stand for the roots of the given and proposed equations respectively, in (1) and we get

$$(y+h)^n + p_1 (y+h)^{n-1} + p_2 (y+h)^{n-2} + \ldots\ldots$$

$$\ldots\ldots + p_{n-1} (y+h) + p_n = 0$$

or, $f(y) \equiv y^n + A_1 y^{n-1} + A_2 y^{n-2} + \ldots\ldots$

$\ldots\ldots + A_{n-1} y + A_n = 0$, say.

Then $y^n + A_1 y^{n-1} + A_2 y^{n-2} + \ldots\ldots + A_{n-1} y + A_n$

$\equiv (x-h)^n + A_1 (x-h)^{n-1} + \ldots\ldots + A_{n-1} (x-h) + A_n$.

Evidently, A_n is the remainder when $f(x-h)$ is divided by $(x-h)$; the quotient is then

$$(x-h)^{n-1} + A_1 (x-h)^{n-2} + \ldots\ldots + A_{n-1}.$$

Again A_{n-1} is the remainder when this is divided by $(x-h)$ and so on. Thus the successive remainders, when $f(x)$ is divided by $(x-h)$, are the successive coefficients of the transformed equation beginning from the end.

If the roots are to be increased by h, then we follow the same process with $y = x + h$.

(iv) Formation of an equation whose roots are the squares of the roots of the given equation.

Replacing x by $(-x)$ in the identity

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots\ldots + p_n$$
$$\equiv (x-\alpha_1)(x-\alpha_2)\ldots\ldots(x-\alpha_n), \quad \ldots (4)$$

we get $x^n - p_1 x^{n-1} + p_2 x^{n-2} - \ldots\ldots + (-1)^n p_n$

$$\equiv (x+\alpha_1)(x+\alpha_2)\ldots\ldots(x+\alpha_n). \quad \ldots (5)$$

Multiplying (4) and (5), we obtain

$$(x^n + p_2 x^{n-2} + \ldots\ldots)^2 - (p_1 x^{n-1} + p_3 x^{n-3} + \ldots\ldots)^2$$
$$= (x^2 - \alpha_1{}^2)(x^2 - \alpha_2{}^2)\ldots\ldots(x^2 - \alpha_n{}^2).$$

Expanding the left hand side and putting $x^2 = y$ on both sides, we get

$$y^n + (2p_2 - p_1{}^2) y^{n-1} + (p_2{}^2 - 2p_1 p_3 + 2p_4) y^{n-2} + \ldots\ldots$$
$$= (y - \alpha_1{}^2)(y - \alpha_2{}^2)\ldots\ldots(y - \alpha_n{}^2).$$

Hence the required equation is

$$y^n + (2p_2 - p_1{}^2) y^{n-1} + (p_2{}^2 - 2p_1 p_3 + 2p_4) y^{n-2} + \ldots\ldots = 0.$$

Note. Putting $y = x^2$, that is, $x = \pm\sqrt{y}$ in (1) and then simplifying after transposing and squaring both sides, we can get the required equation.

(v) Formation of an equation whose roots are the cubes of the roots of the given equation.

Let the given equation (1) be denoted by $f(x) = 0$.

Then $f(x) \equiv (x-\alpha_1)(x-\alpha_2)\cdots\cdots(x-\alpha_n)$.

Replacing x by $\frac{x}{\omega}$ and $\frac{x}{\omega^2}$ successively, where ω is an imaginary cube root of unity, we get

$$f\left(\frac{x}{\omega}\right) \equiv \frac{1}{\omega^n}(x-\omega\alpha_1)(x-\omega\alpha_2)\cdots\cdots(x-\omega\alpha_n)$$

and $$f\left(\frac{x}{\omega^2}\right) \equiv \frac{1}{\omega^{2n}}(x-\omega^2\alpha_1)(x-\omega^2\alpha_2)\cdots\cdots(x-\omega^2\alpha_n).$$

Now $f(x).f\left(\frac{x}{\omega}\right).f\left(\frac{x}{\omega^2}\right) = \frac{1}{\omega^{3n}}(x^3-\alpha_1{}^3)(x^3-\alpha_2{}^3)\cdots\cdots(x^3-\alpha_n{}^3)$

$$= (x^3-\alpha_1{}^3)(x^3-\alpha_2{}^3)\cdots\cdots(x^3-\alpha_n{}^3).$$

Hence, putting $x^3 = y$ in the product on the left hand side and then equating it to zero, we get the required equation.

Note. Putting $y = x^3$, that is , $x = y^{\frac{1}{3}}$ in (1) and then simplifying after transposing and cubing both sides, we can get the required equation.

3.8. Transformation in general .

An equation $f(x) = 0$ is given. We are to form a new equation $g(y) = 0$ in y, whose roots are connected with the roots of the given equation $f(x) = 0$ by a given relation $\phi(x, y) = 0$.

The equation $g(y) = 0$ is obtained by eliminating x between $f(x) = 0$ and $\phi(x, y) = 0$.

3.9. Removal of a term from an equation.

Let the roots of the equation

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots\cdots + a_{n-1}x + a_n = 0$$

be diminished by h. Then the transformed equation is

$$a_0(y+h)^n + a_1(y+h)^{n-1} + a_2(y+h)^{n-2} + \cdots\cdots$$

$$\cdots\cdots + a_{n-1}(y+h) + a_n = 0.$$

Expanding by Binomial theorem for positive integral index, we get

$$a_0\{y^n + ny^{n-1}h + \tfrac{1}{2}n(n-1)y^{n-2}h^2 + \cdots\cdots\}$$

$$+ a_1\{y^{n-1} + (n-1)y^{n-2}h + \cdots\cdots\}$$

$$+ a_2(y^{n-2} + \cdots\cdots) + \cdots\cdots + a_n = 0.$$

Collecting the coefficients of like powers of y, we have

$$a_0 y^n + (na_0 h + a_1) y^{n-1} + \{\tfrac{1}{2} n(n-1) a_0 h^2 + (n-1) a_1 h + a_2\} y^{n-2} + \cdots\cdots + a_n = 0.$$

Now, to remove the second term of the transformed equation, we put

$$na_0 h + a_1 = 0, \text{ that is, } h = \frac{-a_1}{na_0}.$$

Thus, to remove the second term, we are to increase the roots of the given equation by $\frac{a_1}{na_0}$.

Similarly, if the third term is to be removed, then we have to choose h such that

$$\tfrac{1}{2} n(n-1) a_0 h^2 + (n-1) a_1 h + a_2 = 0,$$

which obviously gives two values of h.

Note. Standard methods of solving a cubic or a biquadratic require removal of some terms.

3.10. Equation of squared differences of a cubic.

Let us form an equation whose roots are the squares of the differences of every two roots of a given cubic. For this, we consider the cubic

$$x^3 + qx + r = 0, \qquad \ldots \quad (1)$$

in which the second term is absent and to which a general cubic equation can easily be reduced.

Let α, β, γ be the roots of the equation (1).

We have to form an equation in y whose roots will be

$$(\beta - \gamma)^2, (\gamma - \alpha)^2 \text{ and } (\alpha - \beta)^2.$$

Assuming y to be equal to any one of the roots of the required transformed equation, say, $(\beta - \gamma)^2$, we have

$$y = (\beta - \gamma)^2 = \beta^2 + \gamma^2 - 2\beta\gamma = \alpha^2 + \beta^2 + \gamma^2 - \alpha^2 - 2\frac{\alpha\beta\gamma}{\alpha}. \qquad \ldots \quad (2)$$

Now, since α, β, γ are the roots of the equation (1), we have

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \beta\gamma + \gamma\alpha = q \text{ and } \alpha\beta\gamma = -r.$$

Therefore $\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = -2q.$

Thus, from (2), we get $y = -2q - \alpha^2 + \frac{2r}{\alpha}$.

Hence the required transformation connecting x and y becomes

$$y = -2q - x^2 + \frac{2r}{x}$$

or, $x^3 + (y + 2q)\,x - 2r = 0.$ ... (3)

Subtracting (1) from (3), we have

$$(y + q)\,x - 3r = 0, \quad \text{giving} \quad x = \frac{3r}{y+q}.$$

Substituting this value of x in (1), we have the required equation as

$$\left(\frac{3r}{y+q}\right)^3 + q\left(\frac{3r}{y+q}\right) + r = 0$$

or, $r(y+q)^3 + 3rq(y+q)^2 + (3r)^3 = 0$

or, $(y+q)^3 + 3q(y+q)^2 + 27r^2 = 0$

or, $y^3 + 6qy^2 + 9q^2y + (4q^3 + 27r^2) = 0.$ ... (4)

Now, if it be required to form an equation whose roots are the squares of the differences of the roots α, β, γ of the cubic

$$ax^3 + 3bx^2 + 3cx + d = 0,\ a \neq 0,$$ ... (5)

then we first remove the second term of this cubic, the resulting equation being

$$y^3 + \frac{3H}{a^2}y + \frac{G}{a^3} = 0,$$ ... (6)

where $H = ac - b^2$, $G = a^2d - 3abc + 2b^3$.

Since the difference of any two roots remains the same by the removal of the second term, the required equation will be the same as the equation of squared differences of (6).

Now, comparing (1) and (6), we have

$$q = \frac{3H}{a^2} \text{ and } r = \frac{G}{a^3}.$$

Thus, putting for q and r in (4), we get the required equation as

$$y^3 + \frac{18H}{a^2}y^2 + \frac{81H^2}{a^4}y + \frac{27}{a^6}(G^2 + 4H^3) = 0,$$ ... (7)

whose roots are $(\beta - \gamma)^2$, $(\gamma - \alpha)^2$ and $(\alpha - \beta)^2$.

Multiplying the roots of this equation by a^2, we can put the equation (7) in the form which is free from fractions as

$$y^3 + 18Hy^2 + 81H^2 y + 27(G^2 + 4H^3) = 0. \quad \ldots \quad (8)$$

The roots of this equation are

$$a^2(\beta-\gamma)^2, a^2(\gamma-\alpha)^2, a^2(\alpha-\beta)^2.$$

Cor. We have, from (8),

$$a^6(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2 = -27(G^2+4H^3).$$

Now $G^2 + 4H^3 = (a^2 d - 3abc + 2b^3)^2 + 4(ac - b^2)^3$

$$= a^2(a^2 d^2 - 6abcd + 4ac^3 + 4b^3 d - 3b^2 c^2)$$

$$= a^2 \Delta,$$

where Δ stands for the expression in the parentheses.

Therefore $a^4(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2 = -27\Delta$.

The expression Δ is the discriminant of the cubic (5) and its vanishing is the necessary and sufficient condition that the equation (5) will have two equal roots.

If, in addition, $G = H = 0$, that is, if $\frac{a}{b} = \frac{b}{c} = \frac{c}{d}$, then three roots of the cubic (5) are identical.

3.11. Nature of the roots of a cubic.

(a) The equation of the cubic is $x^3 + qx + r = 0$.

If one root of the equation of the squared differences of a cubic be zero, then two roots of the given equation are equal. Hence, from equation (4) of the previous article, we see that if $27r^2 + 4q^3 = 0$, then the transformed equation has one root zero and hence the equation $x^3 + qx + r = 0$ has two equal roots.

If α, β, γ be real, then $(\beta-\gamma)^2, (\gamma-\alpha)^2, (\alpha-\beta)^2$ are all positive. Hence $(27r^2 + 4q^3)$ is negative. Thus, in order that the equation $x^3 + qx + r = 0$ may have all its roots real, $(27r^2 + 4q^3)$ must be negative, that is, $\left(\frac{r}{2}\right)^2 + \left(\frac{q}{3}\right)^3$ must be negative.

On the other hand, if $(27r^2 + 4q^3)$ be positive, then the transformed equation has a negative root and therefore the original equation $x^3 + qx + r = 0$ must have two imaginary roots ; for, only a pair of imaginary roots can produce a negative root of the transformed equation.

Hence, if $27r^2+4q^3=0$, then the cubic has three real roots but not distinct; if $27r^2+4q^3<0$, then all the three roots are real and distinct; if $27r^2+4q^3>0$, then two roots are imaginary.

(*b*) *The equation of the cubic is* $ax^3+3bx^2+3cx+d=0$.

We know that the equation of the squared differences of this cubic is

$$F(y)\equiv y^3+\frac{18H}{a^2}y^2+\frac{81H^2}{a^4}y+\frac{27}{a^6}(G^2+4H^3)=0, \quad \ldots (1)$$

where $H=ac-b^2$ and $G=a^2d-3abc+2b^3$.

If α, β, γ be the roots of the given cubic, then the roots of the cubic (1) are $(\beta-\gamma)^2, (\gamma-\alpha)^2, (\alpha-\beta)^2$.

If α, β, γ be all real, then the roots of the cubic (1) are all positive.

If α be real and β, γ be imaginary, being of the form $(u+iv)$ and $(u-iv)$, where $v\neq 0$, then $(\beta-\gamma)^2=-4v^2<0$.

Thus two imaginary roots of the given cubic assert the existence of one negative root of the squared differences of the cubic.

Now consider the following three cases :

I. $G^2+4H^3<0$.

Since G and H are real and $G^2>0$, hence $H<0$.

Now $F(-y)=-y^3+\frac{18H}{a^2}y^2-\frac{81H^2}{a^4}y+\frac{27}{a^6}(G^2+4H^3)$.

There being no change of sign, $F(y)=0$ has no negative root and hence the roots of the given equation are all real.

II. $G^2+4H^3=0$.

Either (*i*) $G=H=0$, *or* (*ii*) both G and H are different from zero.

(*i*) If $G=H=0$, then all the roots of the cubic are identical and since one root is real, all the three roots must be real.

(*ii*) If $G\neq 0$, $H\neq 0$, then two of the roots of the given cubic are equal and hence all the three roots are real.

III. $G^2+4H^3>0$.

In this case, $F(-\infty)=-\infty$ and $F(0)>0$.

Hence $F(y)=0$ must have a negative root and hence the given cubic has two imaginary roots and one real root.

3.12. Illustrative Examples.

Ex. 1. *Find an equation whose roots are the roots of the equation*

$$x^7 + 3x^5 + x^3 - x^2 + 7x + 2 = 0,$$

with their signs changed.

Put $x = -y$ in the given equation. The transformed equation is

$$(-y)^7 + 3(-y)^5 + (-y)^3 - (-y)^2 + 7(-y) + 2 = 0$$

or, $-y^7 - 3y^5 - y^3 - y^2 - 7y + 2 = 0$

or, $y^7 + 3y^5 + y^3 + y^2 + 7y - 2 = 0$.

Ex. 2. *Change the equation* $3x^4 - 4x^3 + 4x^2 - 2x + 1 = 0$ *into another, the coefficient of whose highest term will be unity.*

In this case,we see that if we multiply the roots by 3, then the coefficient of the highest degree term will be one. To do this, we give the transformation

$$x = \tfrac{1}{3}y.$$

The transformed equation is

$$3\left(\frac{y}{3}\right)^4 - 4\left(\frac{y}{3}\right)^3 + 4\left(\frac{y}{3}\right)^2 - 2\left(\frac{y}{3}\right) + 1 = 0$$

or, $\frac{y^4}{27} - \frac{4}{27}y^3 + \frac{4}{9}y^2 - \frac{2}{3}y + 1 = 0$

or, $y^4 - 4y^3 + 12y^2 - 18y + 27 = 0$.

Ex. 3. *Remove the fractional coefficients of the equation*

$$2x^3 - \tfrac{3}{2}x^2 - \tfrac{1}{8}x + \tfrac{3}{16} = 0.$$

Let us first give the transformation $x = \frac{y}{a}$.

The transformed equation is

$$\frac{2}{a^3}y^3 - \frac{3}{2a^2}y^2 - \frac{1}{8a}y + \frac{3}{16} = 0$$

or, $2y^3 - \frac{3a}{2}y^2 - \frac{1}{8}a^2y + \frac{3}{16}a^3 = 0$.

If we put $a = 4$, then the coefficients become integral.

Thus putting $a = 4$, we get

$$2y^3 - 6y^2 - 2y + 12 = 0$$

or, $y^3 - 3y^2 - y + 6 = 0$.

Ex. 4. *Find the equation whose roots are the reciprocals of the roots of the equation*

$$x^3 + px^2 + qx + r = 0.$$

Changing x to y^{-1}, we get

$\frac{1}{y^3}+p\frac{1}{y^2}+q\frac{1}{y}+r=0$, that is, $ry^3+qy^2+py+1=0$.

Ex. 5. (*a*) *Diminish the roots of* $2x^3-15x^2+31x-12=0$ *by* 1.

(*b*) *Find the equation each of whose roots is greater by* 2 *than a root of the equation* $x^3-5x^2+6x-3=0$.

(*a*) The arrangement is as follows :

$x-1$	2	-15	31	-12
		2	-13	18
	2	-13	18	6
		2	-11	
	2	-11	7	
		2		
	2	-9		
	2			

The transformed equation is $2y^3-9y^2+7y+6=0$.

(*b*) $x+2$

	1	-5	6	-3
		-2	14	-40
	1	-7	20	-43
		-2	18	
	1	-9	38	
		-2		
	1	-11		
	1			

The transformed equation is $y^3-11y^2+38y-43=0$.

Ex. 6. *Remove the second term of the equation* $x^3+6x^2+12x-19=0$ *and solve the given equation.*

Let us transform the equation by putting $x=y+h$.

Therefore $(y+h)^3+6(y+h)^2+12(y+h)-19=0$

or, $y^3+3y^2h+3yh^2+h^3+6y^2+12yh+6h^2+12y+12h-19=0$

or, $y^3+3(h+2)y^2+3(h^2+4h+4)y+(h^3+6h^2+12h-19)=0$.

We shall have to put $h=-2$ to remove the second term.

The transformed equation is thus $y^3-27=0$, the roots of which are $3, 3\omega, 3\omega^2$, where ω and ω^2 are the imaginary cube roots of unity.

But $x=y+h=y-2$.

Therefore $x=3-2, 3\omega-2, 3\omega^2-2=1, \frac{1}{2}(-7\pm3\sqrt{3}\,i)$.

Ex. 7. *Find the equation whose roots are the squares of the roots of the equation* $x^4 - 2x^3 + 3x^2 - x + 7 = 0$.

If $\alpha, \beta, \gamma, \delta$ be the roots of the given equation, we have the identity

$$x^4 - 2x^3 + 3x^2 - x + 7 \equiv (x-\alpha)(x-\beta)(x-\gamma)(x-\delta). \quad \ldots \quad (1)$$

Let us put $(-x)$ for x in this identity. Thus we get

$$x^4 + 2x^3 + 3x^2 + x + 7 \equiv (x+\alpha)(x+\beta)(x+\gamma)(x+\delta). \quad \ldots \quad (2)$$

Multiplying (1) and (2), we get

$$(x^4 + 3x^2 + 7)^2 - (2x^3 + x)^2 = (x^2-\alpha^2)(x^2-\beta^2)(x^2-\gamma^2)(x^2-\delta^2).$$

Putting y for x^2, we have

$$(y^2 + 3y + 7)^2 - y(2y+1)^2 = (y-\alpha^2)(y-\beta^2)(y-\gamma^2)(y-\delta^2).$$

Hence the equation, whose roots are $\alpha^2, \beta^2, \gamma^2, \delta^2$, is

$$(y^2 + 3y + 7)^2 - y(2y+1)^2 = 0$$

or, $y^4 + 2y^3 + 19y^2 + 41y + 49 = 0$.

Second method :

Putting $y = x^2$, that is, $x = \pm\sqrt{y}$ in the given equation, we get

$$y^2 \mp 2y\sqrt{y} + 3y \mp \sqrt{y} + 7 = 0$$

or, $y^2 + 3y + 7 = \pm(2y\sqrt{y} + \sqrt{y})$.

Squaring both sides, we get

$$y^4 + 9y^2 + 49 + 6y^3 + 14y^2 + 42y = 4y^3 + 4y^2 + y$$

or, $y^4 + 2y^3 + 19y^2 + 41y + 49 = 0$.

This is the required equation.

Ex. 8. *If α, β, γ be the roots of the equation $x^3 - px^2 + qx - r = 0$, then form the equation whose roots are*

(*i*) $\beta\gamma + \frac{1}{\alpha}, \ \gamma\alpha + \frac{1}{\beta}, \ \alpha\beta + \frac{1}{\gamma}$. [*T. H. 2008*]

(*ii*) $\alpha^2 + \beta^2 - \gamma^2, \ \beta^2 + \gamma^2 - \alpha^2, \ \gamma^2 + \alpha^2 - \beta^2$.

Here we have $\alpha + \beta + \gamma = p$, $\alpha\beta + \beta\gamma + \gamma\alpha = q$, $\alpha\beta\gamma = r$.

(*i*) Let $y = \beta\gamma + \frac{1}{\alpha} = \frac{\alpha\beta\gamma + 1}{\alpha} = \frac{r+1}{\alpha}$. Therefore $\alpha = \frac{r+1}{y}$.

Now, since α is a root of the given equation, we have

$$\alpha^3 - p\alpha^2 + q\alpha - r = 0$$

or, $\left(\frac{r+1}{y}\right)^3 - p\left(\frac{r+1}{y}\right)^2 + q\left(\frac{r+1}{y}\right) - r = 0$

or, $ry^3 - q(r+1)y^2 + p(r+1)^2 y - (r+1)^3 = 0$.

This is the required equation.

(*ii*) Let $y = \alpha^2 + \beta^2 - \gamma^2 = \Sigma\alpha^2 - 2\gamma^2$

$= (\Sigma\alpha)^2 - 2\Sigma\alpha\beta - 2\gamma^2 = p^2 - 2q - 2\gamma^2.$

Therefore $2\gamma^2 = p^2 - 2q - y$.

Now, since γ is a root of the given equation, we have

$$\gamma^3 - p\gamma^2 + q\gamma - r = 0$$

or, $$\gamma(\gamma^2 + q) - (p\gamma^2 + r) = 0$$

or, $$\gamma^2(\gamma^2 + q)^2 = (p\gamma^2 + r)^2.$$

Substituting for γ^2, we get the required equation as

$$\tfrac{1}{2}(p^2 - 2q - y)\left\{\tfrac{1}{2}(p^2 - 2q - y) + q\right\}^2 = \left\{\frac{p}{2}(p^2 - 2q - y) + r\right\}^2$$

or, $$\left(t - \frac{y}{2}\right)\left(t - \frac{y}{2} + q\right)^2 = \left\{p\left(t - \frac{y}{2}\right) + r\right\}^2, \text{ where } t = \frac{p^2 - 2q}{2}.$$

Ex. 9. *If* α, β, γ *be the roots of the equation* $x^3 + px^2 + qx + r = 0$, *then find the equation whose roots are*

$$\beta^2 + \beta\gamma + \gamma^2,\ \gamma^2 + \gamma\alpha + \alpha^2,\ \alpha^2 + \alpha\beta + \beta^2.$$

Let y be such that

$$y = \beta^2 + \beta\gamma + \gamma^2 = (\alpha^2 + \beta^2 + \gamma^2) - \alpha^2 + \frac{\alpha\beta\gamma}{\alpha}$$

$$= \{(\alpha + \beta + \gamma)^2 - 2\Sigma\alpha\beta\} - \alpha^2 + \frac{\alpha\beta\gamma}{\alpha}.$$

Now, α, β, γ being the roots of the given equation,

$$\alpha + \beta + \gamma = -p,\ \alpha\beta + \beta\gamma + \gamma\alpha = q,\ \alpha\beta\gamma = -r.$$

Hence $$y = (p^2 - 2q) - \alpha^2 - \frac{r}{\alpha}$$

or, $$\alpha y = (p^2 - 2q)\alpha - \alpha^3 - r. \quad \ldots (1)$$

But α is a root of the given equation,

therefore $$0 = \alpha^3 + p\alpha^2 + q\alpha + r. \quad \ldots (2)$$

α-eliminant of (1) and (2) will give us the transformed equation.

Thus, adding (1) and (2), we have

$$\alpha y = (p^2 - q)\alpha + p\alpha^2. \quad \ldots (3)$$

Now $\alpha \neq 0$; therefore $$\alpha = \frac{y + q - p^2}{p}.$$

Substituting this value of α in (2), we get

$$\frac{(y+q-p^2)^3}{p^3}+\frac{(y+q-p^2)^2}{p}+\frac{q(y+q-p^2)}{p}+r=0$$

or, $y^3+(3q-2p^2)y^2+(3q^2-3qp^2+p^4)y+(q^3-q^2p^2+rp^3)=0$.

This is the required transformed equation.

Ex. 10. *If* α, β, γ *be the roots of the equation* $x^3+px^2+qx+r=0$, *then*

(*a*) *form the equation whose roots are* $\alpha+\frac{1}{\alpha}, \beta+\frac{1}{\beta}, \gamma+\frac{1}{\gamma}$;

(*b*) *find the value of* $\left(\frac{1}{\beta}+\frac{1}{\gamma}-\frac{1}{\alpha}\right)\left(\frac{1}{\gamma}+\frac{1}{\alpha}-\frac{1}{\beta}\right)\left(\frac{1}{\alpha}+\frac{1}{\beta}-\frac{1}{\gamma}\right)$.

[*N. B. H. 1983; B. H. 1991*]

(*a*) Here we have the identity

$$x^3+px^2+qx+r\equiv(x-\alpha)(x-\beta)(x-\gamma). \quad \ldots \quad (1)$$

Changing x to $\frac{1}{x}$, we get, after simplification,

$$rx^3+qx^2+px+1\equiv r\left(x-\frac{1}{\alpha}\right)\left(x-\frac{1}{\beta}\right)\left(x-\frac{1}{\gamma}\right). \quad \ldots \quad (2)$$

Multiplying (1) and (2) and dividing both sides by x^3, we get

$$r\left(x^3+\frac{1}{x^3}\right)+(pr+q)\left(x^2+\frac{1}{x^2}\right)+(p+pq+qr)\left(x+\frac{1}{x}\right)+(1+p^2+q^2+r^2)$$
$$\equiv r\left\{\left(x+\frac{1}{x}\right)-\left(\alpha+\frac{1}{\alpha}\right)\right\}\left\{\left(x+\frac{1}{x}\right)-\left(\beta+\frac{1}{\beta}\right)\right\}\left\{\left(x+\frac{1}{x}\right)-\left(\gamma+\frac{1}{\gamma}\right)\right\}.$$

Now, putting $x+\frac{1}{x}=y$, we get the required equation as

$$r(y^3-3y)+(pr+q)(y^2-2)+(p+pq+qr)y+(1+p^2+q^2+r^2)=0$$

or, $ry^3+(pr+q)y^2+(p+pq+qr-3r)y+(p-r)^2+(q-1)^2=0$.

(*b*) Let us form the equation whose roots are

$$\frac{1}{\beta}+\frac{1}{\gamma}-\frac{1}{\alpha}, \frac{1}{\gamma}+\frac{1}{\alpha}-\frac{1}{\beta}, \frac{1}{\alpha}+\frac{1}{\beta}-\frac{1}{\gamma}.$$

We have

$$\frac{1}{\beta}+\frac{1}{\gamma}-\frac{1}{\alpha}=\frac{1}{\alpha}+\frac{1}{\beta}+\frac{1}{\gamma}-\frac{2}{\alpha}=\frac{\beta\gamma+\gamma\alpha+\alpha\beta}{\alpha\beta\gamma}-\frac{2}{\alpha}=-\frac{q}{r}-\frac{2}{\alpha}.$$

We put $y=-\frac{q}{r}-\frac{2}{\alpha}$.

Therefore $\frac{\alpha}{2}=\frac{-r}{q+yr}$, whence $\alpha=\frac{-2r}{ry+q}$.

Since α is a root of the given equation,

therefore $\alpha^3 + p\alpha^2 + q\alpha + r = 0$

or, $-\frac{8r^3}{(ry+q)^3} + \frac{4pr^2}{(ry+q)^2} - \frac{2qr}{(ry+q)} + r = 0$

or, $8r^3 - 4pr^2(ry+q) + 2qr(ry+q)^2 - r(ry+q)^3 = 0$.

The required value is the product of the roots of this equation and is

$$\frac{8r^3 - 4pqr^2 + 2q^3r - q^3r}{r^4} = \frac{1}{r^3}(8r^2 - 4pqr + q^3).$$

Ex. 11. *Find the equation whose roots are the squares of the differences of the roots of the cubic* $x^3 - 7x - 6 = 0$.

Let α, β, γ be the roots of the given cubic. Then we have

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \beta\gamma + \gamma\alpha = -7 \quad \text{and} \quad \alpha\beta\gamma = 6.$$

Now we are to form an equation whose roots are

$$(\beta - \gamma)^2, (\gamma - \alpha)^2, (\alpha - \beta)^2.$$

Let $y = (\beta - \gamma)^2 = \beta^2 + \gamma^2 - 2\beta\gamma$

$$= \alpha^2 + \beta^2 + \gamma^2 - \alpha^2 - \frac{2\alpha\beta\gamma}{\alpha}$$

$$= \{(\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha)\} - \alpha^2 - \frac{2\alpha\beta\gamma}{\alpha}$$

$$= 14 - \alpha^2 - \frac{12}{\alpha}$$

or, $\alpha y = 14\alpha - \alpha^3 - 12$. ... (1)

Since α is a root of the given equation, we have

$$0 = \alpha^3 - 7\alpha - 6. \quad \ldots \quad (2)$$

Adding (1) and (2), we get

$$\alpha y = 7\alpha - 18$$

or, $\alpha = -\frac{18}{y-7}$.

Thus, putting this value of α in (2), we get

$$-\left(\frac{18}{y-7}\right)^3 + 7\left(\frac{18}{y-7}\right) - 6 = 0$$

or, $6(y-7)^3 - 126(y-7)^2 + (18)^3 = 0$

or, $(y-7)^3 - 21(y-7)^2 + 972 = 0$

or, $y^3 - 42y^2 + 441y - 400 = 0$.

This is the required equation.

Ex. 12. *Form the equation of squared differences of*

$$x^3 + 6x^2 + 9x + 4 = 0$$

and hence solve it. [*C. H. 1976*]

Let us first remove the second term of the given cubic. If h be the quantity by which the roots of the given equation should be diminished, then h is given by

$a_0 nh + a_1 = 0$, that is, $h + 2 = 0$, in the present case.

Thus $h = -2$, that is, the roots are to be increased by 2.

The scheme of synthetic division is as follows :

-2	1	6	9	4
		-2	-8	-2
	1	4	1	2
		-2	-4	
	1	2	-3	
		-2		
	1	0		

The transformed equation is thus $z^3 - 3z + 2 = 0$. ... (1)

Since the difference of any two roots remains the same by this transformation, the equation of squared differences of the given equation will be the same as that of the equation (1).

Now, proceeding as in the previous example, if α, β, γ be the roots of the equation (1), then

$$\alpha + \beta + \gamma = 0, \quad \alpha\beta + \beta\gamma + \gamma\alpha = -3 \quad \text{and} \quad \alpha\beta\gamma = -2.$$

Hence $y = (\beta - \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 - \alpha^2 - \dfrac{2\alpha\beta\gamma}{\alpha} = 6 - \alpha^2 + \dfrac{4}{\alpha}$

or, $\alpha y = 6\alpha - \alpha^3 + 4.$ ... (2)

Since α is a root of the equation (1), we have

$$0 = \alpha^3 - 3\alpha + 2. \quad \ldots \quad (3)$$

Adding (2) and (3), we have $\alpha y = 3\alpha + 6$.

Hence $\alpha = \dfrac{6}{y - 3}$

Substituting this value of α in (3), we get the required equation as

$$\left(\frac{6}{y-3}\right)^3 - 3\left(\frac{6}{y-3}\right) + 2 = 0$$

or, $2(y-3)^3 - 18(y-3)^2 + 216 = 0$

or, $y^3 - 18y^2 + 81y = 0$ or, $y(y-9)^2 = 0.$

Therefore 0, 9, 9 are the roots of this equation.

Thus the roots of the equation (1) are

$$\frac{6}{0-3}, \frac{6}{9-3}, \frac{6}{9-3}, \text{ that is, } -2, 1, 1.$$

Hence the roots of the given equation are $-4, -1, -1$, as $h = -2$.

Note. Notice that one root of the transformed equation is zero and hence two roots of the given equation are equal.

Examples III(C)

1. Find the equations whose roots are

(*i*) double the roots of $x^4 - 3x^3 + 2x^2 + 4x - 1 = 0$;

(*ii*) four times the roots of $3x^4 + 4x^3 - 7x^2 + 4x - 9 = 0$.

2. Find the equations whose roots are the roots of the following equations with their signs changed :

(*i*) $x^4 + 5x^3 - 6x^2 + 8x - 9 = 0$,

(*ii*) $x^7 - 3x^5 + 5x^2 + 6x - 8 = 0$,

(*iii*) $x^6 + 3x^5 - 4x^4 + 3x^3 + 2x^2 - 1 = 0$.

3. Remove the fractional coefficients of the following equations :

(*i*) $x^3 - \frac{1}{2}x^2 + \frac{2}{3}x - 1 = 0$.

(*ii*) $x^4 - \frac{1}{3}x^3 + \frac{2}{9}x^2 - \frac{4}{27}x + \frac{2}{81} = 0$.

(*iii*) $x^4 + \frac{5}{6}x^3 - \frac{13}{18}x - \frac{7}{48} = 0$.

(*iv*) $x^5 - \frac{7}{2}x^4 - \frac{5}{3}x^3 + \frac{7}{54}x^2 + \frac{5}{288} = 0$.

4. Transform the following equations to one with unity as its leading coefficient :

(*i*) $3x^4 - 5x^3 + x^2 - x + 1 = 0$.

(*ii*) $4x^4 + 3x^3 - 4x^2 - 5x + 2 = 0$.

(*iii*) $5x^5 - 10x^4 - 2x^3 + 25x^2 + 23 = 0$.

(*iv*) $8x^4 + 16x^3 - 12x^2 + 15x - 7 = 0$.

5. Form the equation with integral coefficients (with unity as its leading coefficient) whose roots are $1, (-\frac{1}{2})$ and 5.

6. Diminish the roots of the equations

(*i*) $x^3 + x - 2 = 0$ by 2;

(*ii*) $x^4 - 5x^3 + 7x^2 - 17x + 11 = 0$ by 4;

(*iii*) $x^5 - 4x^4 + 3x^2 - 4x + 6 = 0$ by 3.

7. (*a*) Find the equation whose roots are the roots of the equation $x^4 - 3x^3 + 2x^2 + 7x - 5 = 0$, each diminished by 2.

(*b*) If α, β, γ be the roots of the equation $4x^3 - 8x^2 - 19x + 38 = 0$, then find the equation whose roots are $\alpha - 2, \beta - 2, \gamma - 2$. Solve the obtained equation and from it find the roots of the original equation. [*C. H. 1998*]

8. Increase the roots of the equations

(*i*) $4x^5 - 2x^3 + 7x - 3 = 0$ by 2;

(*ii*) $x^3 + x - 2 = 0$ by 3;

(*iii*) $3x^4 + 7x^3 - 15x^2 + x - 2 = 0$ by 7;

(*iv*) $4x^4 + 32x^3 + 83x^2 + 76x + 21 = 0$ by 2. [*K. H. 1979*]

9. (*a*) Remove the second terms of the equations:

(*i*) $x^4 + 8x^3 + x - 5 = 0$,

(*ii*) $x^3 + 6x^2 + 12x - 9 = 0$,

(*iii*) $x^4 - 12x^3 + 48x^2 - 72x + 35 = 0$,

(*iv*) $x^4 + 8x^3 + 19x^2 + 12x - 5 = 0$.

(*b*) Remove the second terms of the equations

(*i*) $x^3 + 6x^2 + 9x + 4 = 0$, [*C. H. 1970*]

(*ii*) $x^4 + 4x^3 - 7x^2 - 22x + 24 = 0$ [*C. H. 1977; V. H. 1990*]

and hence solve the equations.

(*c*) Removing the second term of the equation $x^4 + 8x^3 + 18x^2 + 8x - 10 = 0$, use Descartes' rule of signs to deduce that the given equation has two imaginary roots. [*C. H. 2004*]

(*d*) Remove the third term of the equation

$$x^4 - 4x^3 - 18x^2 - 3x + 2 = 0.$$

10. Find the condition that the second and the fourth terms of the equation $a_0x^4 + 4a_1x^3 + 6a_2x^2 + 4a_3x + a_4 = 0$ should be capable of being removed by the same transformation of the form $x = y + h$. [*C. H. 1976*]

11. (*a*) Form the equations whose roots are the reciprocals to those of the equations

(*i*) $x^5 + 6x^4 - 7x^3 + 8x^2 + 9x + 2 = 0$,

(*ii*) $x^4 - 4x^3 + 5x^2 - 8x + 5 = 0$,

(*iii*) $x^3 + 2x^2 - 2 = 0$.

(*b*) Solve the equation $15x^4 - 16x^3 - 56x^2 + 64x - 16 = 0$, given that the roots are in H.P.

[If the given equation be $f(x) = 0$, the roots of $f(1/x) = 0$ are in A.P.]

(*c*) Find the condition that the roots of the equation $x^4+px^3+qx^2+rx+s=0$ are in H. P.

(*d*) If $\alpha,\beta,\gamma,\delta$ be the roots of the equation $sx^4+rx^3+qx^2+px+1=0$ and if $\frac{1}{\beta}+\frac{1}{\gamma}=\frac{1}{\alpha}+\frac{1}{\delta}$, then find a relation among p, q, r, s. [*C. H. 1994*]

12. If α,β,γ be the roots of the equation $x^3-3x^2+8x-5=0$; then form an equation whose roots are $2\alpha+3,\ 2\beta+3,\ 2\gamma+3$.

[Multiply the roots by 2 and then increase by 3.]

13. Find the equations whose roots are the squares of the roots of the equations

(*i*) $x^3+p_1x^2+p_2x+p_3=0$,

(*ii*) $x^4+px^3+qx^2+rx+s=0$,

(*iii*) $x^3-x^2+2x-3=0$,

(*iv*) $x^3-x^2+8x-6=0$,

(*v*) $x^3+3x^2+3x-7=0$,

14. (*a*) Finding the equation whose roots are the squares of the roots of the equation $x^4-x^3+2x^2-x+1=0$, use Descartes' rule of signs to deduce that the given equation has no real root. [*C. H. 1988*]

(*b*) The equation whose roots are the squares of the roots of the cubic $x^3-ax^2+bx-1=0$ is found to be identical with this cubic. Prove that *either* (*i*) $a=b=0$; (*ii*) $a=b=3$;

or a, b are the roots of the equation $x^2+x+2=0$. [*C. H. 1987*]

(*c*) If α, β, γ be the roots of the equation $x^3+x-3=0$, then show that the equation, whose roots are $\alpha^2+2,\ \beta^2+2,\ \gamma^2+2$, is

$$y^3-4y^2+5y-11=0.$$

15. Find the equations whose roots are the cubes of the roots of the equations

(*i*) $x^4-2x^3+x^2+3x-1=0$,

(*ii*) $x^3+2x^2+3x+1=0$.

16. If α,β,γ be the roots of the equation $2x^3+x^2+x+1=0$, then find the equation whose roots are

(*i*) $\alpha^{-3},\ \beta^{-3},\ \gamma^{-3}$. (*ii*) $\frac{1+\alpha}{1-\alpha},\ \frac{1+\beta}{1-\beta},\ \frac{1+\gamma}{1-\gamma}$.

(*iii*) $\beta^{-3}+\gamma^{-3}-\alpha^{-3},\ \gamma^{-3}+\alpha^{-3}-\beta^{-3},\ \alpha^{-3}+\beta^{-3}-\gamma^{-3}$.

17. If α, β, γ be the roots of the equation $x^3 + 2x^2 + 3x + 4 = 0$, then find the equation whose roots are

(i) $1+\frac{1}{\alpha}, 1+\frac{1}{\beta}, 1+\frac{1}{\gamma}$.

(ii) $\left(\alpha - \frac{1}{\beta\gamma}\right), \left(\beta - \frac{1}{\gamma\alpha}\right), \left(\gamma - \frac{1}{\alpha\beta}\right)$. [C. H. 1980]

18. (a) If α, β, γ be the roots of the equation $2x^3 + 3x^2 - x - 1 = 0$, then find the equation whose roots are

(i) $\frac{\alpha}{\beta+\gamma}, \frac{\beta}{\gamma+\alpha}, \frac{\gamma}{\alpha+\beta}$. (ii) $\frac{1}{1-\alpha}, \frac{1}{1-\beta}, \frac{1}{1-\gamma}$.

(b) If α, β, γ be the roots of the equation $x^3 - 2x^2 + x - 3 = 0$, then form the equation whose roots are $\alpha\beta, \beta\gamma, \gamma\alpha$.

19. (a) If the roots of the cubic $x^3 + 2x^2 + 3x + 1 = 0$ be α, β, γ, then find the equation whose roots are

$$\frac{1}{\beta^2}+\frac{1}{\gamma^2}-\frac{1}{\alpha^2}, \frac{1}{\gamma^2}+\frac{1}{\alpha^2}-\frac{1}{\beta^2}, \frac{1}{\alpha^2}+\frac{1}{\beta^2}-\frac{1}{\gamma^2}.$$

(b) If α, β, γ be the roots of the equation $x^3 + 2x^2 + 1 = 0$, then find the equation whose roots are

(i) $\alpha+\frac{1}{\alpha}, \beta+\frac{1}{\beta}, \gamma+\frac{1}{\gamma}$. [C. H. 1986]

(ii) $\alpha + \beta\gamma, \beta + \gamma\alpha, \gamma + \alpha\beta$.

(c) If α, β, γ be the roots of the equation $x^3 - px^2 + r = 0$, then find the equation whose roots are $\frac{\beta+\gamma}{\alpha}, \frac{\gamma+\alpha}{\beta}, \frac{\alpha+\beta}{\gamma}$. [N. B. H. 2007]

(d) If α, β, γ be the roots of the equation $x^3 + 3x + 1 = 0$, then find the equation whose roots are $\left(\frac{\alpha}{\beta}+\frac{\beta}{\alpha}\right), \left(\frac{\beta}{\gamma}+\frac{\gamma}{\beta}\right), \left(\frac{\gamma}{\alpha}+\frac{\alpha}{\gamma}\right)$ and hence find the value of $\sum\left(\frac{\alpha}{\beta}+\frac{\beta}{\alpha}\right)$.

20. If α, β, γ be the roots of the cubic $x^3 + px - q = 0$, then find the equation whose roots are

(i) $\alpha^2 + \beta^2, \beta^2 + \gamma^2, \gamma^2 + \alpha^2$.

(ii) $\frac{\beta+\gamma}{\alpha^2}, \frac{\gamma+\alpha}{\beta^2}, \frac{\alpha+\beta}{\gamma^2}$. (iii) $\frac{\beta^2+\gamma^2}{\alpha^2}, \frac{\gamma^2+\alpha^2}{\beta^2}, \frac{\alpha^2+\beta^2}{\gamma^2}$.

21. The roots of the cubic $x^3 + qx + r = 0$ are α, β, γ. Form the equation whose roots are

(i) $\beta^2 + \beta\gamma + \gamma^2, \gamma^2 + \gamma\alpha + \alpha^2, \alpha^2 + \alpha\beta + \beta^2$.

(ii) $l\alpha + m\beta\gamma, l\beta + m\gamma\alpha, l\gamma + m\alpha\beta$.

22. If α, β, γ be the roots of the cubic $x^3+px^2+qx-r=0$, then find the equation whose roots are $\beta\gamma+\frac{1}{\alpha}$, $\gamma\alpha+\frac{1}{\beta}$, $\alpha\beta+\frac{1}{\gamma}$.

Hence find the value of $\Sigma\left(\beta\gamma+\frac{1}{\alpha}\right)$ and $\left(\beta\gamma+\frac{1}{\alpha}\right)\left(\gamma\alpha+\frac{1}{\beta}\right)\left(\alpha\beta+\frac{1}{\gamma}\right)$.

23. If α, β, γ be the roots of the cubic $x^3-px^2+qx-r=0$, then find the equation whose roots are

(*i*) $\beta+\gamma$, $\gamma+\alpha$, $\alpha+\beta$.

(*ii*) $\frac{1}{\beta}+\frac{1}{\gamma}$, $\frac{1}{\gamma}+\frac{1}{\alpha}$, $\frac{1}{\alpha}+\frac{1}{\beta}$.

(*iii*) $\frac{\alpha}{\beta+\gamma-\alpha}$, $\frac{\beta}{\gamma+\alpha-\beta}$, $\frac{\gamma}{\alpha+\beta-\gamma}$. [*B. H. 1969*]

(*iv*) $\alpha\beta+\alpha\gamma$, $\alpha\beta+\beta\gamma$, $\beta\gamma+\gamma\alpha$.

24. If α, β, γ be the roots of the equation $x^3+px^2+qx+r=0$, then

(*i*) find the equation whose roots are

$$\frac{\alpha}{\beta+\gamma}, \frac{\beta}{\gamma+\alpha}, \frac{\gamma}{\alpha+\beta};$$

hence find the value of $\Sigma\frac{\alpha\beta}{(\beta+\gamma)(\gamma+\alpha)}$;

(*ii*) find the equation whose roots are $\beta\gamma-\alpha^2$, $\gamma\alpha-\beta^2$, $\alpha\beta-\gamma^2$.

Hence find the condition that the roots of the given equation will be in G.P.

25. (*a*) If α, β, γ be the roots of the equation $ax^3+bx^2+cx+d=0$, then find the equation whose roots are

(*i*) $\alpha+\beta-\gamma$, $\beta+\gamma-\alpha$, $\gamma+\alpha-\beta$.

(*ii*) $2\alpha-\beta-\gamma$, $2\beta-\gamma-\alpha$, $2\gamma-\alpha-\beta$.

(*b*) If α, β, γ be the roots of the cubic

$$x^3-3px^2+3(p-1)x+1=0,$$

then find the equation whose roots are $(1-\alpha), (1-\beta), (1-\gamma)$.

Deduce that α, β, γ are all real, if p be real. [*C. H. 1986*]

[The equation whose roots are $(1-\alpha), (1-\beta), (1-\gamma)$ has also roots $\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\gamma}$.]

26. If α be a root of the cubic $x^3 - 3x + 1 = 0$, then show that the other roots are $(\alpha^2 - 2)$ and $(2 - \alpha - \alpha^2)$.

[The substitution $y = x^2 - 2$ transforms the equation into itself.]

27. If $\alpha, \beta, \gamma, \delta$ be the roots of the equation $x^4 + px^2 + q = 0, q \neq 0$, then find the values of $\Sigma\alpha^{-4}$ and $\Sigma\alpha^{-2}\beta^{-2}$.

Also find the equation whose roots are

$$\beta+\gamma+\delta-\alpha,\ \gamma+\delta+\alpha-\beta,\ \delta+\alpha+\beta-\gamma,\ \alpha+\beta+\gamma-\delta.$$

28. If α, β, γ be the roots of the equation

$$x^3 + px^2 + qx + r = 0,$$

then prove that the equation in y whose roots are

$$\frac{\beta\gamma - \alpha^2}{\beta+\gamma-2\alpha},\ \frac{\gamma\alpha - \beta^2}{\gamma+\alpha-2\beta},\ \frac{\alpha\beta - \gamma^2}{\alpha+\beta-2\gamma}$$

is obtained by the homogeneous transformation

$$3xy + p(x+y) + q = 0.$$

29. Find the equation whose roots are the six ratios of the roots of the cubic $x^3 + qx + r = 0, r \neq 0$.

30. Find the equations whose roots are the squared differences of the roots of the cubics

(*i*) $x^3 - 13x - 12 = 0$,

(*ii*) $x^3 - 27x + 54 = 0$,

(*iii*) $x^3 + 6x^2 + 7x + 2 = 0$,

(*iv*) $3x^3 - 11x^2 + 8x + 4 = 0$.

31. Find the equation of the squared differences of the roots of the cubic $x^3 + x^2 - x = 1$. Hence show that two roots of this equation are equal.

32.(*a*) If α, β, γ be the roots of the cubic $x^3 - 9x + 9 = 0$, then show that $(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha) = \pm 27$.

(*b*) If α, β, γ be the roots of the equation

$$x^3 - 3(1+a+a^2)x + (1+3a+3a^2+2a^3) = 0,$$

then show that $(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2 = 81(1+a+a^2)^2$. [*V. H. 2009*]

(*c*) If $\alpha, \beta, \gamma, \delta$ be the roots of the biquadratic

$$x^4 - x^3 + 2x^2 + x + 1 = 0,$$

then show that $(\alpha^3+1)(\beta^3+1)(\gamma^3+1)(\delta^3+1) = 16$.

Answers

1. (*i*) $y^4 - 6y^3 + 8y^2 + 32y - 16 = 0$.

(*ii*) $3y^4 + 16y^3 - 112y^2 + 256y - 2304 = 0$.

2. (*i*) $y^4 - 5y^3 - 6y^2 - 8y - 9 = 0$.

(*ii*) $y^7 - 3y^5 - 5y^3 + 6y + 8 = 0$.

(*iii*) $y^6 - 3y^5 - 4y^4 - 3y^3 + 2y^2 - 1 = 0$.

3. (*i*) $y^3 - 3y^2 + 24y - 216 = 0$.

(*ii*) $y^4 - y^3 + 2y^2 - 4y + 2 = 0$.

(*iii*) $y^4 + 5y^3 - 156y - 189 = 0$.

(*iv*) $y^5 - 21y^4 - 60y^3 + 28y^2 + 135 = 0$.

4. (*i*) $y^4 - 5y^3 + 3y^2 - 9y + 27 = 0$.

(*ii*) $y^4 + 3y^3 - 16y^2 - 80y + 128 = 0$.

(*iii*) $y^5 - 10y^4 - 10y^3 + 625y^2 + 14375 = 0$

(*iv*) $y^4 + 4y^3 - 6y^2 + 15y - 14 = 0$.

5. $y^3 - 11y^2 + 8y + 20 = 0$.

6. (*i*) $y^3 + 6y^2 + 13y + 8 = 0$.

(*ii*) $y^4 + 11y^3 + 43y^2 + 55y - 9 = 0$.

(*iii*) $y^5 + 11y^4 + 42y^3 + 57y^2 - 13y - 60 = 0$.

7. (*a*) $y^4 + 5y^3 + 8y^2 + 11y + 9 = 0$. (*b*) $4y^3 + 16y^2 - 3y = 0$; $2, \pm\frac{1}{2}\sqrt{19}$.

8. (*i*) $4y^5 - 40y^4 + 158y^3 - 308y^2 + 303y - 129 = 0$.

(*ii*) $y^3 - 9y^2 + 28y - 32 = 0$.

(*iii*) $3y^4 - 77y^3 + 720y^2 - 2876y + 4058 = 0$.

(*iv*) $4y^4 - 13y^2 + 9 = 0$.

9. (*a*) (*i*) $y^4 - 24y^2 + 65y - 55 = 0$. (*ii*) $y^3 - 17 = 0$.

(*iii*) $y^4 - 6y^2 + 8 = 0$. (*iv*) $y^4 - 5y^2 - 1 = 0$.

(*b*) (*i*) $-4, -1, -1$. (*ii*) $1, 2, -3, -4$.

(*d*) $y^4 + 8y^3 - 111y - 196 = 0$ or $y^4 - 8y^3 + 17y - 8 = 0$.

10. $2a_1^3 = 3a_0 a_1 a_2 - a_0^2 a_3$.

11. (*a*) (*i*) $2y^5 + 9y^4 + 8y^3 - 7y^2 + 6y + 1 = 0$.

(*ii*) $5y^4 - 8y^3 + 5y^2 - 4y + 1 = 0$.

(*iii*) $2y^3 - 2y - 1 = 0$.

(*b*) $-2, 2, \frac{2}{3}, \frac{2}{5}$. (*c*) $r^3 + 8ps^2 = 4qrs$, $(qr - ps)(11ps - qr) = 25r^2 s$.

(*d*) $p^3 = 4pq - 8r$.

12. $y^3 - 15y^2 + 95y - 217 = 0$.

13. (i) $y^3+y^2(2p_2-p_1{}^2)+y(p_2{}^2-2p_1p_3)-p_3{}^2=0$.
(ii) $(y^2+qy+s)^2=y(py+r)^2$. (iii) $y^3+3y^2-2y-9=0$.
(iv) $y^3+15y^2+52y-36=0$. (v) $y^3-3y^2+51y-49=0$.

15. (i) $y^4+7y^3+37y^2+30y-1=0$. (ii) $y^3-7y^2+12y+1=0$.

16. (i) $y^3+4y^2+7y+8=0$. (ii) $5y^3-3y^2+7y-1=0$.
(iii) $y^3+4y^2+12y-16=0$.

17. (i) $4y^3-9y^2+8y-2=0$. (ii) $16y^3+40y^2+75y+125=0$.

18. (a) (i) $2y^3+27y^2-6y-4=0$. (ii) $3y^3-11y^2+9y-2=0$.
(b) $y^3-y^2+6y-9=0$.

19. (a) $y^3+12y^2-172y-2072=0$.
(b) (i) $y^3+2y^2-y+2=0$. (ii) $y^3+2y^2+5y+8=0$.
(c) $ry^3+3ry^2+(3r-p^3)y+r=0$. (d) $(y+1)^3+27(y+2)=0$; (-3).

20. (i) $y^3+4py^2+5p^2y+2p^3+q^2=0$ (ii) $qy^3+py^2+1=0$.
(iii) $q^2y^3+(2p^3+3q^2)y^2-(4p^3-3q^2)y+(2p^3+q^2)=0$.

21. (i) $(y+q)^3=0$.
(ii) $y^3-mqy^2+(l^2q+3lmr)y+l^3r-l^2mq^2-2lm^2qr-m^3r^2=0$.

22. $ry^3-q(1+r)y^2-p(1+r)^2y-(1+r)^3=0$; $\frac{q(1+r)}{r}$; $\frac{(1+r)^3}{r}$.

23. (i) $y^3-2py^2+(p^2+q)y+(r-pq)=0$.
(ii) $r^2y^3-2qry^2+(pr+q^2)y+r-pq=0$.
(iii) $(p^3-4pq+8r)y^3+(p^3-4pq+12r)y^2+(6r-pq)y+r=0$.
(iv) $y^3-2qy^2+(q^2+pr)y+r(r-pq)=0$.

24. (i) $y^3(r-pq)+y^2(3r-2pq+p^3)+y(3r-pq)+r=0$; $\frac{3r-pq}{r-pq}$.
(ii) $y^3+(p^2-3q)y^2+(3q^2-p^2q)y+(p^3r-q^3)=0$; $p^3r=q^3$.

25. (a) (i) $a^3y^3+a^2by^2+a(4ac-b^2)y+(4abc-8a^2d-b^3)=0$.
(ii) $a^3y^3+3a(3ac-b^2)y+(27a^2d-9abc+2b^3)=0$.
(b) $y^3+3(p-1)y^2-3py+1=0$.

27. $\frac{2(p^2-2q)}{q^2}$; $\frac{p^2+2q}{q^2}$; $y^4+4py^2+16q=0$.

29. $r^2(y^2+y+1)^3+q^3y^2(y+1)^2=0$.

30. (i) $y^3-78y^2+1521y-4900=0$.
(ii) $y^3-162y^2+6561y=0$.
(iii) $y^3-30y^2+225y-68=0$.
(iv) $81y^3-882y^2+2401y=0$.

31. $y^3-8y^2+16y=0$.

4 THEORY OF EQUATIONS (3)

4.1. Reciprocal equations.

An equation is said to be a *reciprocal equation*, if the reciprocal of any root of the equation be also a root of the same equation.

A reciprocal equation remains unaltered by changing x by $\frac{1}{x}$.

Let the equation be

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots\ldots + p_{n-1} x + p_n = 0 , p_n \neq 0 . \quad \ldots \quad (1)$$

Then the equation, whose roots are the reciprocals of the roots of the given equation, is

$$\left(\frac{1}{x}\right)^n + p_1 \left(\frac{1}{x}\right)^{n-1} + p_2 \left(\frac{1}{x}\right)^{n-2} + \ldots\ldots + p_{n-1} \left(\frac{1}{x}\right) + p_n = 0 .$$

Multiplying both sides by x^n, we get

$$p_n x^n + p_{n-1} x^{n-1} + \ldots\ldots + p_1 x + 1 = 0 . \quad \ldots \quad (2)$$

If (1) be a reciprocal equation, then (1) and (2) will represent the same equation. Hence

$$\frac{p_{n-1}}{p_n} = p_1 , \frac{p_{n-2}}{p_n} = p_2 , \ldots\ldots , \frac{1}{p_n} = p_n . \quad \ldots \quad (3)$$

The last relation of (3) gives $p_n^2 = 1$,

that is, $p_n = \pm 1 .$ $\quad \ldots \quad (4)$

(*i*) If $p_n = 1$, then we have, from the remaining relations of (3),

$$p_{n-1} = p_1 , p_{n-2} = p_2 , \ldots\ldots , p_1 = p_{n-1} .$$

Thus this type of reciprocal equations will be such that the coefficients of corresponding terms taken from the beginning and the end are equal in magnitude with same sign.

These are called *reciprocal equations of the first type,* or *of the first class,* or *of the first kind.*

(*ii*) If $p_n = -1$, then we have, from the remaining relations of (3),

$$p_{n-1} = -p_1 , p_{n-2} = -p_2 , \ldots\ldots , p_1 = -p_{n-1} .$$

Thus this type of reciprocal equations will be such that the coefficients of the corresponding terms taken from the beginning and the end are equal in magnitude but opposite in signs.

These are called *reciprocal equations of the second type*, or *of the second class*, or *of the second kind.*

In a reciprocal equation of second type, if the degree be even, say, $n = 2m$, then one of the conditions becomes

$$p_m = -p_m \text{ , that is , } p_m = 0.$$

Thus *the middle term of a reciprocal equation of second type and of even degree is absent.*

4.2. Reduction of a reciprocal equation.

It is clear from the definition that if α be a root of a reciprocal equation, then $\frac{1}{\alpha}$ must also be a root of the equation. Thus the roots of a reciprocal equation occur in pairs such as $\alpha, \frac{1}{\alpha}; \beta, \frac{1}{\beta}$; etc.

If the degree of the equation be *odd*, then the equation must have a root which is its own reciprocal, that is, either 1 or (-1). It is observed by substitution that in a first type equation of odd degree (-1) is a root, while for an odd degree equation of second type 1 is a root.

Division by $(x+1)$ in the former case and by $(x-1)$ in the latter case, leaves a reciprocal equation of first type and of even degree.

A reciprocal equation of second type and of even degree, say $2m$, may be written as

$$x^{2m} - 1 + p_1 x (x^{2m-2} - 1) + \cdots\cdots = 0 .$$

This equation , as is obvious, is satisfied by both 1 and (-1).

By dividing by $(x^2 - 1)$, this equation is also reducible to a reciprocal equation of first type and of even degree.

Thus all reciprocal equations can be reduced to those of first type whose degree is even. An even degree first type reciprocal equation is called the *standard form* of reciprocal equation.

We prove below formally two theorems in connection with the reduction and solution of reciprocal equations.

Theorem 1. *The solution of any reciprocal equation depends on that of a standard reciprocal equation.*

Let $f(x)=p_0x^n+p_1x^{n-1}+p_2x^{n-2}+\cdots\cdots+p_n=0$ be a reciprocal equation. If this equation be of first type, then

$$x^n f\left(\frac{1}{x}\right)=f(x).$$

Now, let n be odd and equal to $(2m+1)$. Then

$$f(x)=p_0(x^{2m+1}+1)+p_1x(x^{2m-1}+1)+\cdots\cdots+p_mx^m(x+1)=0.$$

Thus $f(x)$ is divisible by $(x+1)$. Let $\phi(x)$ be the quotient when $f(x)$ is divided by $(x+1)$. Then

$$x^{2m}\phi\left(\frac{1}{x}\right)=x^{2m}\frac{f\left(\frac{1}{x}\right)}{\frac{1}{x}+1}=x^{2m+1}\cdot\frac{f\left(\frac{1}{x}\right)}{1+x}=\frac{f(x)}{x+1}=\phi(x).$$

Hence $\phi(x)=0$ is a reciprocal equation of first type and of degree $2m$.

If again the equation $f(x)=0$ be of second type, then

$$x^n f\left(\frac{1}{x}\right)=-f(x).$$

Let n be odd and equal to $(2m+1)$. Then grouping the terms as above, it is seen that $f(x)$ is divisible by $(x-1)$.

If then $\phi(x)$ be the quotient when $f(x)$ is divided by $(x-1)$, as before $x^{2m}\phi\left(\frac{1}{x}\right)=\phi(x)$.

Thus $\phi(x)=0$ is a reciprocal equation of first type and of degree $2m$.

Furthermore, if n be even and equal to $2m$, since $p_r=-p_{2m-r}$, then it follows that $p_m=-p_m$ and hence $p_m=0$. Thus the equation may be written as

$$f(x)=p_0(x^{2m}-1)+p_1x(x^{2m-2}-1)+\cdots\cdots+p_{m-1}x^{m-1}(x^2-1)=0.$$

Thus $f(x)$ is divisible by (x^2-1).

Let $\phi(x)$ be the quotient when $f(x)$ is divided by (x^2-1).

Then

$$x^{2m-2}\phi\left(\frac{1}{x}\right)=x^{2m-2}\cdot\frac{f\left(\frac{1}{x}\right)}{x^{-2}-1}=-x^{2m}\cdot\frac{f\left(\frac{1}{x}\right)}{x^2-1}=\frac{f(x)}{x^2-1}=\phi(x).$$

Hence $\phi(x)=0$ is a reciprocal equation of first type and of even degree.

Thus, in all cases, the solution of $f(x)=0$ depends on that of an equation of first type and of even degree.

Theorem 2. *A reciprocal equation of the standard form can always be depressed to another of half the dimension.*

Let us consider the equation

$$p_0 x^{2m}+p_1 x^{2m-1}+\ldots\ldots+p_1 x+p_0=0,$$

which is a reciprocal equation of first type and of even degree.

Dividing both sides of the equation by x^m, we get

$$p_0\left(x^m+\frac{1}{x^m}\right)+p_1\left(x^{m-1}+\frac{1}{x^{m-1}}\right)+\ldots\ldots+p_m=0. \qquad \ldots \quad (1)$$

Let us assume $x+\frac{1}{x}=z$ and write $x^p+\frac{1}{x^p}=V_p$ for brevity.

Then we have $V_1=z$, $V_2=\left(x+\frac{1}{x}\right)^2-2=z^2-2$, etc.

Also we have $\left(x+\frac{1}{x}\right)\left(x^{p-1}+\frac{1}{x^{p-1}}\right)$

$$=\left(x^p+\frac{1}{x^p}\right)+\left(x^{p-2}+\frac{1}{x^{p-2}}\right),$$

which gives $zV_{p-1}=V_p+V_{p-2}$,

that is, $V_p=zV_{p-1}-V_{p-2}$.

Putting $2, 3, 4, 5, \ldots\ldots$ for p in succession, we have

$$V_2=zV_1-V_0=z^2-2,$$

$$V_3=zV_2-V_1=z^3-3z,$$

$$V_4=zV_3-V_2=z^4-4z^2+2,$$

$$V_5=zV_4-V_3=z^5-5z^3+5z, \text{ and so on.}$$

Thus, putting these in (1), we get an equation in z.

Generally, $\left(x^m+\frac{1}{x^m}\right)$ is of m dimension in z and hence the equation in z is of half the dimension.

Now, if z_1 be a root of this equation, then x can be obtained by solving the quadratic

$$x+\frac{1}{x}=z_1,$$

that is, $$x^2-z_1x+1=0.$$

4.3. Illustrative Examples.

Ex. 1. *Solve the reciprocal equation* $x^4+10x^3+26x^2+10x+1=0$.

This is a reciprocal equation of first type.

Dividing both sides of the equation by x^2, we get

$$x^2+10x+26+\frac{10}{x}+\frac{1}{x^2}=0$$

or, $$\left(x^2+\frac{1}{x^2}\right)+10\left(x+\frac{1}{x}\right)+26=0.$$

Putting $x+\frac{1}{x}=z$, we get $x^2+\frac{1}{x^2}=\left(x+\frac{1}{x}\right)^2-2=z^2-2$.

Therefore the equation becomes

$$z^2-2+10z+26=0$$

or, $$z^2+10z+24=0$$

or, $$(z+6)(z+4)=0.$$

Thus $z=-6$ or -4.

Now we are to solve the equations

$$x+\frac{1}{x}=-6 \quad \text{and} \quad x+\frac{1}{x}=-4,$$

that is, $x^2+6x+1=0$ and $x^2+4x+1=0$.

The roots of the given equation are thus

$$-3\pm2\sqrt{2},-2\pm\sqrt{3}.$$

Ex. 2. *Reduce the reciprocal equation* $x^5-6x^4+7x^3+7x^2-6x+1=0$ *to its standard form and solve it.*

The given equation is a first type reciprocal equation of odd degree. To reduce this to the standard form, that is, to a reciprocal equation of first type and of even degree, we are to divide it by $(x+1)$ as it is seen, by substitution, that (-1) is a root of the given equation. Thus the required equation of the standard form will be

$$x^4-7x^3+14x^2-7x+1=0.$$

To reduce this equation to half its dimension, we divide both sides of this equation by x^2 and get

$$x^2-7x+14-\frac{7}{x}+\frac{1}{x^2}=0,$$

that is, $$\left(x^2+\frac{1}{x^2}\right)-7\left(x+\frac{1}{x}\right)+14=0.$$

Putting $x+\frac{1}{x}=z$, we reduce this equation as

$$z^2-2-7z+14=0$$

or, $$z^2-7z+12=0,$$

which gives $z=4$ or 3.

Now, solving the equations $x+\frac{1}{x}=4$ and $x+\frac{1}{x}=3$, we get the roots as

$$x=2\pm\sqrt{3} \text{ and } x=\tfrac{1}{2}(3\pm\sqrt{5}).$$

Thus the roots of the given equation are

$$-1, 2\pm\sqrt{3}, \tfrac{1}{2}(3\pm\sqrt{5}).$$

Ex. 3. *Solve the equation* $x^5-5x^4+9x^3-9x^2+5x-1=0$. [*C. H. 1991*]

This is a reciprocal equation of second type and of odd degree. Further more, by substitution, we see that 1 is a root of this equation. Dividing both sides of the given equation by $(x-1)$, we have

$$x^4-4x^3+5x^2-4x+1=0,$$

which is a reciprocal equation of the standard type.

Dividing both sides by x^2, we get

$$\left(x^2+\frac{1}{x^2}\right)-4\left(x+\frac{1}{x}\right)+5=0.$$

Now, putting $x+\frac{1}{x}=z$, we reduce this equation as

$$z^2-2-4z+5=0$$

or, $$z^2-4z+3=0,$$

which gives $z=3$ or 1, that is, $x+\frac{1}{x}=3$ or $x+\frac{1}{x}=1$.

These give $x=\frac{1}{2}(3\pm\sqrt{5})$ or $x=\frac{1}{2}(1\pm i\sqrt{3})$.

Hence the roots of the given equation are

$$1, \tfrac{1}{2}(3\pm\sqrt{5}), \tfrac{1}{2}(1\pm i\sqrt{3}).$$

Ex. 4. *Solve the equation*

$$6x^6 - 25x^5 + 31x^4 - 31x^2 + 25x - 6 = 0.$$ [*C. H. 1978, 1998*]

This is a reciprocal equation of second type and of even degree. Hence the expression on the left will have $(x^2 - 1)$ as a factor. Arranging the equation as

$$6(x^6 - 1) - 25x(x^4 - 1) + 31x^2(x^2 - 1) = 0,$$

we divide both sides of the equation by $(x^2 - 1)$, corresponding to the roots 1 and (-1), to get

$$6x^4 - 25x^3 + 37x^2 - 25x + 6 = 0,$$

which is a reciprocal equation in standard form.

Dividing both sides by x^2, we have

$$6\left(x^2 + \frac{1}{x^2}\right) - 25\left(x + \frac{1}{x}\right) + 37 = 0.$$

Putting $x + \frac{1}{x} = z$, we get

$$6(z^2 - 2) - 25z + 37 = 0$$

or, $$6z^2 - 25z + 25 = 0,$$

which gives $z = \frac{5}{2}$ or $\frac{5}{3}$.

Now, solving the equations

$$x + \frac{1}{x} = \frac{5}{2} \text{ and } x + \frac{1}{x} = \frac{5}{3},$$

we get $x = 2$ or $\frac{1}{2}$ and $x = \frac{1}{6}(5 \pm \sqrt{-11})$.

Thus the roots of the given equation are

$$\pm 1, 2, \frac{1}{2}, \frac{1}{6}(5 \pm \sqrt{-11}).$$

Examples IV (A)

Solve the following equations :

1. $2x^4 - 5x^3 + 4x^2 - 5x + 2 = 0$.
2. $2x^4 + x^3 - 6x^2 + x + 2 = 0$.
3. (*a*) $6x^4 + 35x^3 + 62x^2 + 35x + 6 = 0$. [*N. B. H. 1984*]
   (*b*) $6x^4 - 35x^3 + 62x^2 - 35x + 6 = 0$. [*C. H. 1984*]
   (*c*) $6x^4 + 5x^3 - 38x^2 + 5x + 6 = 0$.
4. (*a*) $x^4 - 8x^3 + 17x^2 - 8x + 1 = 0$. [*C. H. 1965; B. H. 1987*]
   (*b*) $x^4 - 10x^3 + 26x^2 - 10x + 1 = 0$.

5. $x^5+x^4+x^3+x^2+x+1=0$. [*B. H. 1984*]

6. $x^5-5x^4+9x^3-9x^2+5x-1=0$.

7. $x^5-9x^4+25x^3-25x^2+9x-1=0$. [*C. H. 1969*]

8. $x^5-6x^4+7x^3-7x^2+6x-1=0$. [*C. H. 1988*]

9. $2x^5-7x^4-x^3-x^2-7x+2=0$.

10. $2x^5-15x^4+37x^3-37x^2+15x-2=0$.

11. $6x^5-41x^4+97x^3-97x^2+41x-6=0$. [*C. H. 1985*]

12. $6x^5+11x^4-33x^3-33x^2+11x+6=0$. [*T. H. 1989; B. H. 1998*]

13. $4x^6-24x^5+57x^4-73x^3+57x^2-24x+4=0$.

14. $2x^6-x^5-2x^3-x+2=0$. [*B. H. 1990*]

15. Reduce the equation $4x^4-85x^3+357x^2-340x+64=0$ to a reciprocal equation and then solve it. [*N. B. H. 1985*]

16. Show that the equation $x^4-3x^3+4x^2-2x+1=0$ can be transformed into a reciprocal equation by diminishing the roots by unity. Hence solve the equation.

17. (*a*) Show that the transformation of the form $x=2y-1$ transforms the equation $x^4-14x^2-40x-11=0$ into reciprocal form and hence solve the equation.

(*b*) Show that if the roots of the equation $x^4+x^3-4x^2-3x+3=0$ be increased by 2, then the transformed equation is a reciprocal equation. Solve the reciprocal equation and hence obtain the solution of the given equation. [*N. B. H. 2009*]

18. Determine the transformation $x=my+n$ which will change the equation $x^4+5x^3+9x^2+5x-1=0$ into a reciprocal equation and then solve it. [*C. H. 1989*]

19. (*a*) Reduce the equation $3x^6+x^5-27x^4+27x^2-x-3=0$ to a reciprocal equation of the standard form and then solve it. [*C. H. 2006*]

(*b*) Reducing the reciprocal equation

$$x^8-x^6+2x^5-2x^3+x^2-1=0$$

to standard form, find its roots. [*C. H. 2004*]

(*c*) Reduce the reciprocal equation

$$x^{10}-3x^8+5x^6-5x^4+3x^2-1=0$$

to its standard form and solve it.

20. Show that $(x+1)^4+a(x^4+1)=0$ is a reciprocal equation, if $a\neq -1$. Solve it when $a=2$.

Answers

1. $2, \frac{1}{2}, i, -i$.
2. $1, 1, -2, -\frac{1}{2}$.
3. (*a*) $-2, -3, -\frac{1}{2}, -\frac{1}{3}$. (*b*) $2, 3, \frac{1}{2}, \frac{1}{3}$. (*c*) $2, \frac{1}{2}, -3, -\frac{1}{3}$.
4. (*a*) $\frac{1}{2}(3\pm\sqrt{5}), \frac{1}{2}(5\pm\sqrt{21})$. (*b*) $2\pm\sqrt{3}, 3\pm2\sqrt{2}$.
5. $-1, \frac{1}{2}(1\pm\sqrt{3}\,i), \frac{1}{2}(-1\pm\sqrt{3}\,i)$.
6. $1, \frac{1}{2}(1\pm\sqrt{3}\,i), \frac{1}{2}(3\pm\sqrt{5})$.
7. $1, \frac{1}{2}(3\pm\sqrt{5}), \frac{1}{2}(6\pm\sqrt{21})$.
8. $1, \pm i, \frac{1}{2}(5\pm\sqrt{21})$.
9. $-1, 2\pm\sqrt{3}, \frac{1}{4}(1\pm\sqrt{15}\,i)$.
10. $1, 2, \frac{1}{2}, 2\pm\sqrt{3}$.
11. $1, 2, 3, \frac{1}{2}, \frac{1}{3}$.
12. $-1, 2, \frac{1}{2}, -3, -\frac{1}{3}$.
13. $2, 2, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}(1\pm\sqrt{3}\,i)$.
14. $-1, -1, \pm i, \frac{1}{2}(3\pm\sqrt{7}\,i)$.
15. $\frac{1}{4}, 1, 4, 16$.
16. $\frac{1}{4}(3+\sqrt{5}\pm i\sqrt{10+2\sqrt{5}}), \frac{1}{4}(3-\sqrt{5}\pm i\sqrt{10-2\sqrt{5}})$.
17. (*a*) $\sqrt{5}\pm\sqrt{2+2\sqrt{5}}, -\sqrt{5}\pm\sqrt{2-2\sqrt{5}}$. (*b*) $\pm\sqrt{3}, \frac{1}{2}(-1\pm\sqrt{5})$.
18. $x=y-2$; $\frac{1}{4}(-5+\sqrt{5}\pm\sqrt{6\sqrt{5}-2}), \frac{1}{4}(-5-\sqrt{5}\pm i\sqrt{6\sqrt{5}+2})$.
19. (*a*) $\pm1, -3, -\frac{1}{3}, \frac{1}{2}(3\pm\sqrt{5})$. (*b*) $1, -1, -1, -1, -\omega, -\omega, -\omega^2, -\omega^2$.
    (*c*) $\pm1, \frac{1}{2}(\sqrt{3}\pm i), \frac{1}{2}(\sqrt{3}\pm i), \frac{1}{2}(-\sqrt{3}\pm i), \frac{1}{2}(-\sqrt{3}\pm i)$.
20. $\pm i, \frac{1}{3}(-2\pm i\sqrt{5})$.

4.4. Binomial equations.

The most general binomial equation is of the form

$$x^n = a + ib, \qquad \ldots (1)$$

where $i=\sqrt{-1}$ and a, b are real quantities.

Let us put $a = R\cos\alpha$ and $b = R\sin\alpha$; then the above equation becomes

$$x^n = R(\cos\alpha + i\sin\alpha).$$

Now, if $r(\cos\theta + i\sin\theta)$ be a root of this equation, then, by De Moivre's theorem, we have

$$r^n(\cos n\theta + i\sin n\theta) = R(\cos\alpha + i\sin\alpha).$$

Equating the real and the imaginary parts from both sides, we get

$$r^n\cos n\theta = R\cos\alpha \quad \text{and} \quad r^n\sin n\theta = R\sin\alpha.$$

Squaring these two and adding, we get $r^{2n} = R^2$, which gives $r^n = R$ and $\cos n\theta = \cos\alpha,\ \sin n\theta = \sin\alpha$.

Therefore $n\theta = 2k\pi + \alpha$, k being an integer.

Thus $x = R^{\frac{1}{n}}\{\cos(2k\pi+\alpha) + i\sin(2k\pi+\alpha)\}^{\frac{1}{n}}$

$$= R^{\frac{1}{n}}\left\{\cos\frac{1}{n}(2k\pi+\alpha) + i\sin\frac{1}{n}(2k\pi+\alpha)\right\},$$

where $k = 0, 1, 2, \ldots\ldots, (n-1)$.

In particular, if $R = 1$ and $\alpha = 0$, then the equation (1) reduces to $x^n - 1 = 0$,
whose roots are given by

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \text{ where } k = 0, 1, 2, \ldots\ldots, (n-1).$$

Furthermore, if $R = 1$ and $\alpha = \pi$, then the equation (1) reduces to

$$x^n + 1 = 0.$$

The general expression for the roots of this equation is

$$\cos\frac{(2k+1)\pi}{n} + i\sin\frac{(2k+1)\pi}{n},$$

where $k = 0, 1, 2, \ldots\ldots, (n-1)$.

Now the exponent n may be even or odd.

If n be *even*, then the real roots of the binomial equation $x^n - 1 = 0$ are ± 1 and the imaginary roots are

$$\cos\frac{2k\pi}{n} \pm i\sin\frac{2k\pi}{n}, \text{ where } k = 1, 2, \ldots\ldots, (\tfrac{1}{2}n - 1).$$

Now we know $\cos\theta - i\sin\theta = \dfrac{1}{\cos\theta + i\sin\theta}$.

Hence the imaginary roots are the roots of a reciprocal equation $f(x) = 0$, where $f(x)$ is the quotient obtained by dividing $(x^n - 1)$ by $(x^2 - 1)$.

Again, when n is *odd*, the only real root of the equation $x^n - 1 = 0$ is 1 and the imaginary roots are given by

$$\cos\frac{2k\pi}{n} \pm i\sin\frac{2k\pi}{n}, \text{ where } k = 1, 2, \ldots\ldots, \tfrac{1}{2}(n-1).$$

Thus, in this case also, the imaginary roots are the roots of the reciprocal equation $f(x) = 0$, where $f(x)$ is obtained by dividing $(x^n - 1)$ by $(x - 1)$.

Hence *the imaginary roots of a binomial equation are the roots of a reciprocal equation.*

4.5. General properties of binomial equations.

(a) If α be an imaginary root of the equation $x^n - 1 = 0$, then α^m will also be a root, m being an integer.

Since α is a root of the equation $x^n - 1 = 0$, therefore $\alpha^n = 1$.

Therefore $(\alpha^n)^m = 1$, since m is an integer.

Hence $(\alpha^m)^n = 1$, that is, α^m is a root of the equation

$$x^n - 1 = 0 .$$

Cor. The same proposition is true for the equation $x^n + 1 = 0$ but in this case m must be an *odd* integer.

(*b*) *If m and n be prime to each other, then the equations $x^m - 1 = 0$ and $x^n - 1 = 0$ have no common root except unity.*

To prove this property, we take help of the following property of numbers :

If m and n be integers prime to each other, then integers a and b can be found such that

$$mb - na = \pm 1 .$$

This is because of the fact that if $\frac{m}{n}$ be converted into a continued fraction, then $\frac{a}{b}$ is the approximation preceding the final restoration of $\frac{m}{n}$.

Now, if possible, let α be a common root of the given equations

$$x^m - 1 = 0 \text{ and } x^n - 1 = 0 .$$

Then $\alpha^m = 1$ and $\alpha^n = 1$.

Therefore $\alpha^{mb} = 1$ and $\alpha^{na} = 1$.

Dividing, we get $\alpha^{mb - na} = 1$

or, $\alpha^{\pm 1} = 1$.

Therefore $\alpha = 1$.

Thus 1 is the only common root of the two given equations.

(*c*) *If k be the greatest common measure of the two integers m and n, then the roots common to the equations $x^m - 1 = 0$ and $x^n - 1 = 0$ are the roots of the equation $x^k - 1 = 0$.*

Let $m = km'$ and $n = kn'$.

Evidently, m' and n' are prime to each other. Hence integers b and a can be found such that

$$m'b - n'a = \pm 1.$$

Hence $mb - na = \pm k$.

If now α be a common root of the equations $x^m - 1 = 0$ and $x^n - 1 = 0$, then $\alpha^{mb-na} = 1$
or, $\alpha^k = 1$.

Thus α is a root of the equation $x^k - 1 = 0$.

(d) When n is a prime number and α is any imaginary root of the equation $x^n - 1 = 0$, all the roots are included in the series

$$1, \alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}.$$

Since α is a root of the equation $x^n - 1 = 0$,

$$\alpha^0 (= 1), \alpha^1 (= \alpha), \alpha^2, \ldots\ldots, \alpha^{n-1}$$

are all roots of the given equation and they are all different from one another.

If possible, let any two of them, say, α^p and α^q, be equal, where p and q are both less than n. Then, since $\alpha^p = \alpha^q$, we have

$$\alpha^{p-q} = 1.$$

But $(p - q) < n$ and n is necessarily prime to $(p - q)$, so the two equations

$$x^{p-q} - 1 = 0 \text{ and } x^n - 1 = 0$$

cannot have a common root except 1.

Therefore $\alpha^p \neq \alpha^q$,
that is, the roots are all different.

(e) When n is a composite number formed of the factors p, q, r, etc., the roots of the equations

$$x^p - 1 = 0,\ x^q - 1 = 0,\ x^r - 1 = 0, \text{ etc.}$$

all satisfy the equation $x^n - 1 = 0$.

Let α be a root of the equation $x^p - 1 = 0$.

Then $\alpha^p = 1$, $(\alpha^p)^{qr\ldots\ldots} = 1$, that is $\alpha^n = 1$.

Similarly, from the second and the third equations

$$x^q - 1 = 0,\ x^r - 1 = 0,$$

we can show that their roots also satisfy the equation

$$x^n - 1 = 0.$$

(*f*) *When n is a composite number formed of the prime factors p, q, r, etc., the roots of the equation $x^n - 1 = 0$ are the n terms of the product*

$$(1+\alpha+\alpha^2+\cdots\cdots+\alpha^{p-1})(1+\beta+\beta^2+\cdots\cdots+\beta^{q-1})\times (1+\gamma+\gamma^2+\cdots\cdots+\gamma^{r-1})\cdots\cdots,$$

where α is a root of the equation $x^p - 1 = 0$, β of $x^q - 1 = 0$, γ of $x^r - 1 = 0$, etc.

We shall prove this property for three factors p, q, r. The general case can be proved similarly.

We shall show that any term of the product which is of the form $\alpha^a \beta^b \gamma^c$ is a root of the equation $x^n - 1 = 0$.

We have $(\alpha^a)^n = (\alpha^a)^{pqr} = (\alpha^p)^{aqr} = 1$.

Similarly, $(\beta^b)^n = 1$ and $(\gamma^c)^n = 1$.

Hence $(\alpha^a \beta^b \gamma^c)^n - 1 = 0$,

which shows that $\alpha^a \beta^b \gamma^c$ is a root of the equation $x^n - 1 = 0$.

Now we shall show that no two terms of the product are equal.

If possible, let

$$\alpha^a \beta^b \gamma^c = \alpha^{a'} \beta^{b'} \gamma^{c'},$$

that is,

$$\alpha^{a-a'} = \beta^{b'-b} \gamma^{c'-c}.$$

The left hand member of this equation is a root of the equation $x^{p-1} = 0$ and the right hand member is a root of the equation $x^{qr} - 1 = 0$. But, since p and qr are prime to each other, the equations $x^p - 1 = 0$ and $x^{qr} - 1 = 0$ cannot have a common root and hence

$$\alpha^a \beta^b \gamma^c \neq \alpha^{a'} \beta^{b'} \gamma^{c'}.$$

This proves the proposition.

(*g*) *The roots of the equation $x^n - 1 = 0$, where $n = p^a q^b r^c$, and p, q, r are the prime factors of n, are the n products of the form $\alpha\beta\gamma$, where α is a root of the equation $x^{p^a} - 1 = 0$, β is a root of $x^{q^b} - 1 = 0$ and γ is a root of*

$$x^{r^c} - 1 = 0$$

This proposition is an extension of proposition (*f*). Here the prime factors occur more than once in n. The proof is similar.

Any such product of the form $\alpha\beta\gamma$ must be a root, since

$$\alpha^n = 1, \beta^n = 1, \gamma^n = 1, \text{ where } n = p^a q^b r^c.$$

Again, since p^a, q^b, r^c are prime to one another, no two such products as $\alpha\beta\gamma$ can be equal.

Note. A similar proof applies to the general case.

4.6. Special roots of the equation $x^n - 1 = 0$.

Any root of the equation $x^n - 1 = 0$ which is not a root of an equation of the same type and lower degree, is called a *special root* of the equation. This is also called the *special n-th root of unity.*

Thus, if $r < n$ and prime to n, then the special roots of the equation $x^n - 1 = 0$ are $\cos\frac{2r\pi}{n} + i\sin\frac{2r\pi}{n}$.

Obviously, $(n - r)$ is less than n and prime to n.

Therefore $\cos\frac{2(n-r)\pi}{n} + i\sin\frac{2(n-r)\pi}{n}$,

that is to say, $\cos\frac{2r\pi}{n} - i\sin\frac{2r\pi}{n}$ is also a special root of the equation

$$x^n - 1 = 0.$$

Now, if $\alpha = \cos\frac{2r\pi}{n} + i\sin\frac{2r\pi}{n}$ be a special root, then

$$\frac{1}{\alpha} = \cos\frac{2r\pi}{n} - i\sin\frac{2r\pi}{n}$$ is also a special root.

Thus the special roots of an equation can be arranged in pairs such as $\left(\alpha, \frac{1}{\alpha}\right), \left(\beta, \frac{1}{\beta}\right)$, etc.

So *the special roots of an equation are the roots of a reciprocal equation.*

If n be prime, then the number of integers less than n and prime to n is $(n - 1)$. Hence the number of special roots of the equation $x^n - 1 = 0$, in this case, is $(n - 1)$.

Let $n = p^a$, where p is a prime number. Now every divisor of p^a is a divisor of p^{a-1} (except n itself). Therefore any n-th root of the equation belonging to an equation of lower degree than n must belong to the equation

$$x^{p^{a-1}} - 1 = 0.$$

Thus there are $p^a\left(1 - \frac{1}{p}\right)$, that is, $n\left(1 - \frac{1}{p}\right)$ roots belonging to no such equation of lower degree and hence these are the special roots of the equation $x^n - 1 = 0$.

If again $n = p^a q^b$, where p and q are prime to each other, then there are $p^a\left(1-\frac{1}{p}\right)$ and $q^b\left(1-\frac{1}{q}\right)$ special roots of

$x^{p^a}-1=0$ and $x^{q^b}-1=0$ respectively.

Let α and β be the special roots of these equations, then $\alpha\beta$ will be a special root of the equation

$$x^n-1=0.$$

If not, let $(\alpha\beta)^m=1$, where $m<n$.

Now, since $\alpha^m\beta^m=1$, $\alpha^m=\beta^{-m}$.

But α^m is a root of the equation $x^{p^a}-1=0$ and β^{-m} is a root of the equation $x^{q^b}-1=0$.

Now, since p^a and q^b are prime to each other, these equations cannot have a common root except 1. Therefore m cannot be less than n and $\alpha\beta$ is a special root of the equation $x^n-1=0$.

The number of special roots of such an equation is

$$p^a\left(1-\frac{1}{p}\right)q^b\left(1-\frac{1}{q}\right)$$
$$=p^a q^b\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right).$$

Note. The same proof applies to any form of n.

4.7. Two important theorems on special roots.

Theorem 1. *If α be a special root of the equation $x^n-1=0$, then all the roots of the equation are given by the series $1, \alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}$.*

If α be a special root of the given equation, then $\alpha, \alpha^2, \ldots\ldots$ are all roots. Now it can be shown that no two of these are equal.

Let, if possible, $\alpha^p=\alpha^q$. Then $\alpha^{p-q}=1$, where $p-q<n$. Thus α is a root of an equation of the same type and lower degree. But it cannot be, since α is a special root of the given equation. Hence $\alpha^p\neq\alpha^q$.

Theorem 2. *If α be a special root of the equation $x^n-1=0$, then α^p, where p is prime to n and less than it, is also a special root of the equation.*

If α be a special root of the equation $x^n-1=0$, then we know that all the roots $1, \alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}$ are different roots of the equation. Now, from this set, let us select one root α^p, where p is prime to n. We shall show that α^p is a special root of the equation.

Let us consider the roots

$$\alpha^p, \alpha^{2p}, \alpha^{3p}, \ldots\ldots, \alpha^{(n-1)p}, \alpha^{np} (=1).$$

Now, when the exponents of α of this series are divided by n, different remainders are obtained in each case and they are $0, 1, 2, \ldots\ldots, (n-1)$ in some order. This series of roots is the same as the series $1, \alpha, \alpha^2, \ldots\ldots, \alpha^{n-1}$ arranged in different order.

Furthermore, if α^p be a root of an equation of lower degree than n, say, $x^m - 1 = 0$, then $\alpha^{mp} = 1$. This shows that there are two roots equal to 1 in the series. Thus the series does not represent all the roots of the equation and hence α^p cannot be a root of an equation of similar type and lower degree. Therefore α^p is a special root of the equation.

Cor. 1. If α be any special root of the equation $x^n - 1 = 0$, then the complete set of special roots is $\alpha^a, \alpha^b, \alpha^c, \ldots\ldots$, where $a, b, c, \ldots\ldots$ are numbers less than n and prime to it, including unity.

Cor. 2. If α be a special root of the equation $x^p - 1 = 0$ and β be a special root of the equation $x^q - 1 = 0$, then $\alpha\beta$ is a special root of the equation $x^{pq} - 1 = 0$, where p, q are prime to each other.

4.8. Illustrative Examples.

Ex. 1. *Find the special roots of the equation* $x^6 - 1 = 0$. [*C. H. 1980, 1988*]

The special roots of the equation $x^6 - 1 = 0$ are $\cos\frac{2r\pi}{6} + i\sin\frac{2r\pi}{6}$, where r is a positive integer less than 6 and prime to 6. The integers less than 6 and prime to 6 are 1 and 5.

Therefore the special roots are

$$\cos\frac{\pi}{3} + i\sin\frac{\pi}{3} \text{ and } \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}, \text{ that is, } \tfrac{1}{2}(1 \pm i\sqrt{3}).$$

Second method :

The exponent of x in the given binomial equation is 6.

Now $6 = 2 \times 3$.

1, 2 and 3 are the prime factors of 6. Therefore the roots of the equations $x - 1 = 0$, $x^2 - 1 = 0$ and $x^3 - 1 = 0$ are the roots of the equation

$$x^6 - 1 = 0.$$

Now we have $\frac{x^6 - 1}{x^3 - 1} = x^3 + 1$.

Further, dividing $(x^3 + 1)$ by $\frac{x^2 - 1}{x - 1}$, that is, by $(x + 1)$, we get

$$\frac{x^3 + 1}{x + 1} = x^2 - x + 1.$$

Hence $x^2-x+1=0$ will give the special roots of the equation $x^6-1=0$.
Solving this equation, we get $\frac{1}{2}(1\pm i\sqrt{3})$ as the special roots.

Alternatively, the lowest commom multiple of $(x-1)$, (x^2-1) and (x^3-1) is $(x^2-1)(x^2+x+1)$.

Dividing (x^6-1) by $(x^2-1)(x^2+x+1)$, we get (x^2-x+1).

Hence $x^2-x+1=0$ will give the special roots.

Ex. 2. *Find the special roots of the equation* $x^{12}-1=0$.

[C. H. 1986; V. H. 2000; N. B.H. 2004]

The special roots of the equation $x^{12}-1=0$ are $\cos\frac{2r\pi}{12}+i\sin\frac{2r\pi}{12}$, where r is a positive integer less than 12 and prime to 12.

The integers less than 12 and prime to 12 are 1, 5, 7 and 11.

Hence the required special roots are $\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}$, $\cos\frac{5\pi}{6}+i\sin\frac{5\pi}{6}$,

$$\cos\frac{7\pi}{6}+i\sin\frac{7\pi}{6} \text{ and } \cos\frac{11\pi}{6}+i\sin\frac{11\pi}{6},$$

that is, $\cos\frac{\pi}{6}\pm i\sin\frac{\pi}{6}, -\cos\frac{\pi}{6}\pm i\sin\frac{\pi}{6}$,

that is, $\frac{1}{2}(\sqrt{3}\pm i), \frac{1}{2}(-\sqrt{3}\pm i)$.

Examples IV (B)

1. Solve the equation $x^5-1=0$ and deduce that

$$\cos\frac{\pi}{5}=\frac{\sqrt{5}+1}{4} \text{ and } \cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}.$$

2. (*a*) Show that the special roots of the equation $x^6-1=0$ are also roots of the equation $x^5-x^4+x^3-x^2+x-1=0$. *[C. H. 1974]*

(*b*) Show that all the imaginary roots of the equation $x^7=1$ are its special roots. *[C. H. 2003]*

3. Prove that the special roots of the equation $x^9-1=0$ are the roots of the equation $x^6+x^3+1=0$ and their values are

$$\cos\frac{2r\pi}{9}\pm i\sin\frac{2r\pi}{9}, r=1,2,4. \quad \textit{[B. H. 1986; V. H. 2001]}$$

4. Show that the special roots of the equation $x^{10}-1=0$ are the non-real roots of the equation $x^5+1=0$.

5. If n be a prime number, then show that the special roots of the equation $x^{2n}-1=0$ are the non-real roots of the equation. $x^n+1=0$.

6. Prove that the special roots of the equation $x^{15}-1=0$ are the roots of the equation

$$x^8-x^7+x^5-x^4+x^3-x+1=0.$$

Hence show that the roots of the equation

$x^4-x^3-4x^2+4x+1=0$ are $2\cos\frac{2r\pi}{15}$, $r=1,2,4,7$.

[*V. H. 1991*]

7. Show that the special roots of the equation $x^{16}-1=0$ are

$$\cos\frac{r\pi}{8}\pm i\sin\frac{r\pi}{8},\ r=1,3,5,7.$$

8. Form an equation of 12-th degree whose roots are the special roots of the equation $x^{21}-1=0$ and show that it can be reduced to the equation

$$x^6-x^5-6x^4+6x^3+8x^2-8x+1=0.$$

Show also that the number of special roots of the equation $x^{21}-1=0$ is 12.

9. Find the special roots of the equation $x^{24}-1=0$ and deduce that

$$\cos\frac{\pi}{12}=\frac{\sqrt{3}+1}{2\sqrt{2}} \text{ and } \cos\frac{5\pi}{12}=\frac{\sqrt{3}-1}{2\sqrt{2}}.$$ [*N. B. H. 2006*]

Also show that the number of special roots of the equation $x^{24}-1=0$ is 8.

10. If α be a special root of the equation $x^8-1=0$, then prove that

$$(\alpha+2)(\alpha^2+2)\ldots\ldots(\alpha^7+2)=85$$ [*V. H. 1988; B. H. 1994*]

and $1+3\alpha+5\alpha^2+\ldots\ldots+15\alpha^7=\frac{16}{\alpha-1}$. [*V. H. 2006*]

11. (*a*) If α be a special root of the equation $x^{11}-1=0$, then prove that

$$(\alpha+1)(\alpha^2+1)\ldots\ldots(\alpha^{10}+1)=1.$$ [*C. H. 2006*]

(*b*) Solve the equation $x^{11}-1=0$ and hence deduce that

$\cos\frac{\pi}{11}\cos\frac{2\pi}{11}\cos\frac{3\pi}{11}\cos\frac{4\pi}{11}\cos\frac{5\pi}{11}=\frac{1}{2^5}$. [*Viswa-Bharati Hons. 2007*]

12. If α be an imaginary root of the equation $x^n-1=0$ and n be a prime number, then show that

$$(1-\alpha)(1-\alpha^2)(1-\alpha^3)\ldots\ldots(1-\alpha^{n-1})=n.$$ [*C. H. 1984, 2002*]

5 THEORY OF EQUATIONS (4)

5.1. Standard form of a cubic.

Let the general cubic equation with binomial coefficients be

$$ax^3 + 3bx^2 + 3cx + d = 0, \quad a \neq 0. \qquad \ldots \quad (1)$$

Let α, β, γ be the roots of this equation. To diminish the roots of this equation by h, we put $x = y + h$ and the transformed equation is

$$a(y+h)^3 + 3b(y+h)^2 + 3c(y+h) + d = 0$$

or, $$ay^3 + 3(ah+b)y^2 + 3(ah^2 + 2bh + c)y + (ah^3 + 3bh^2 + 3ch + d) = 0.$$

Next we remove the second term by effecting $ah + b = 0$, so that $h = -\frac{b}{a}$ and the equation becomes

$$y^3 + \frac{3}{a^2}(ac - b^2)y + \frac{1}{a^3}(a^2d - 3abc + 2b^3) = 0.$$

Using the symbols $H = ac - b^2$, $G = a^2d - 3abc + 2b^3$, the transformed equation is

$$y^3 + \frac{3H}{a^2}y + \frac{G}{a^3} = 0. \qquad \ldots \quad (2)$$

The roots of this equation are thus

$$\alpha - h, \quad \beta - h, \quad \gamma - h,$$

that is, $$\alpha + \frac{b}{a}, \quad \beta + \frac{b}{a}, \quad \gamma + \frac{b}{a}.$$

But $\frac{b}{a} = -\frac{\alpha + \beta + \gamma}{3}$; therefore the roots of the equation (2) are

$$\tfrac{1}{3}(2\alpha - \beta - \gamma), \ \tfrac{1}{3}(2\beta - \gamma - \alpha), \ \tfrac{1}{3}(2\gamma - \alpha - \beta).$$

We transform further the equation (2) by multiplying the roots by a on putting $z = ay$. Then the final transformed equation becomes

$$z^3 + 3Hz + G = 0,$$

whose roots are $(a\alpha + b)$, $(a\beta + b)$, $(a\gamma + b)$ and is called the *standard form* of the cubic.

5.2. Cardan's solution of a cubic equation.

Let $ax^3 + 3bx^2 + 3cx + d = 0$ ... (1)

be a cubic equation which, when reduced to the standard form by the transformation $z = ax + b$, is reduced to

$$z^3 + 3Hz + G = 0, \quad \ldots \quad (2)$$

where $H = ac - b^2$ and $G = a^2d - 3abc + 2b^3$.

As a solution of the equation (2), we assume

$$z = u^{\frac{1}{3}} + v^{\frac{1}{3}} = m + n, \text{ where } m = u^{\frac{1}{3}} \text{ and } n = v^{\frac{1}{3}}.$$

Therefore $z^3 = (m+n)^3 = m^3 + n^3 + 3mn(m+n)$

$$= m^3 + n^3 + 3mnz$$

or, $z^3 - 3mnz - (m^3 + n^3) = 0.$ ... (3)

Comparing the equations (2) and (3), we get

$$mn = -H \text{ and } m^3 + n^3 = -G,$$

that is, $m^3n^3 = -H^3$ and $m^3 + n^3 = -G.$

Thus m^3 and n^3 are the roots of the equation

$$t^2 + Gt - H^3 = 0. \quad \ldots \quad (4)$$

Solving this quadratic equation, we get its two roots and let us suppose

$$m^3 = \tfrac{1}{2}(-G + \sqrt{G^2 + 4H^3})$$

and $$n^3 = \tfrac{1}{2}(-G - \sqrt{G^2 + 4H^3}). \quad \ldots \quad (5)$$

As there are three cube roots of any number, let them be, in these cases m, ωm, $\omega^2 m$ and n, ωn, $\omega^2 n$ respectively, where ω and ω^2 are the imaginary cube roots of unity.

Now any value of m may be associated with any value of n giving altogether nine values of $z = m + n$. But these must be so chosen that their product is real as suggested by $mn = -H$. Hence we get three pairs of admissible values of m and n, namely, (m, n), $(\omega m, \omega^2 n)$ and $(\omega^2 m, \omega n)$; for, the product of any other pair is imaginary. Thus we get for z, or in other words, the roots of the equation (2) are

$$(m+n),\ (\omega m + \omega^2 n) \text{ and } (\omega^2 m + \omega n). \quad \ldots \quad (6)$$

Then, from the relation $z = ax + b$, we get the roots of (1).

The above solution is generally known as *Cardan's solution*. Cardan obtained the solution from *Tartaglia*.

Note. That the sum of the roots of the reduced cubic (2) is zero, is also satisfied by this solution. For,

$$(m+n)+(\omega m+\omega^2 n)+(\omega^2 m+\omega n)=0.$$

5.3. Nature of the roots of the cubic.

The quantity (G^2+4H^3) is called the *discriminant* of the cubic (2).

As the nature of the roots does not change by the substitution $z=ax+b$, the nature of the roots of the equation (1) will be the same as those of the equation (2), to which we shall confine our discussion.

(*i*) If $G^2+4H^3>0$, then the roots of (4) are real and from (6), we may conclude that the first root $(m+n)$ of (2) is real and the other two are complex conjugate, namely,

$$-\tfrac{1}{2}(m+n)+\tfrac{1}{2}i\sqrt{3}(m-n) \text{ and } -\tfrac{1}{2}(m+n)-\tfrac{1}{2}i\sqrt{3}(m-n).$$

(*ii*) If $G^2+4H^3=0$, then the roots of (4) are equal, that is, $m=n$. In this case, the roots of (2), as seen from (6), are

$$2m,\ (-m) \text{ and } (-m).$$

Thus all the roots are real, two of them being equal. If further $H=G=0$, then all the roots are real and equal.

(*iii*) If $G^2+4H^3<0$, then the roots of (4) are imaginary and m and n cannot be determined by any arithmetical process.

Note. Cardan's method is used only in the first case to get one real and two complex roots of the cubic.

5.4. Trigonometric solution of the cubic equation.

In the case, when $G^2+4H^3<0$, we write in (5)

$$m^3=a+ib \text{ and } n^3=a-ib,$$

so that

$$a=-\tfrac{1}{2}G \text{ and } ib=\tfrac{1}{2}\sqrt{G^2+4H^3}.$$

Now, let us put $a=r\cos\theta$, $b=r\sin\theta$, so that

$$m^3=r(\cos\theta+i\sin\theta) \text{ and } n^3=r(\cos\theta-i\sin\theta).$$

Then, by De Moivre's theorem, we get the values of m and n as

$$r^{\frac{1}{3}}(\cos\tfrac{1}{3}\theta+i\sin\tfrac{1}{3}\theta),\ r^{\frac{1}{3}}\{\cos\tfrac{1}{3}(\theta+2\pi)+i\sin\tfrac{1}{3}(\theta+2\pi)\},$$

$$r^{\frac{1}{3}}\{\cos\tfrac{1}{3}(\theta+4\pi)+i\sin\tfrac{1}{3}(\theta+4\pi)\}$$

and $r^{\frac{1}{3}}(\cos\tfrac{1}{3}\theta-i\sin\tfrac{1}{3}\theta),\ r^{\frac{1}{3}}\{\cos\tfrac{1}{3}(\theta+2\pi)-i\sin\tfrac{1}{3}(\theta+2\pi)\},$

$$r^{\frac{1}{3}}\{\cos\tfrac{1}{3}(\theta+4\pi)-i\sin\tfrac{1}{3}(\theta+4\pi)\}.$$

Thus the roots of the cubic (2), as given by $z = m + n$, are

$$2r^{\frac{1}{3}} \cos \tfrac{1}{3}\theta,\ 2r^{\frac{1}{3}} \cos \tfrac{1}{3}(\theta + 2\pi) \text{ and } 2r^{\frac{1}{3}} \cos \tfrac{1}{3}(\theta + 4\pi),$$

which are all real, $r^{\frac{1}{3}}$ being given by the arithmetical cube root of

$$r = \sqrt{a^2 + b^2} = \sqrt{-H^3}\ .$$

5.5. Illustrative Examples.

Ex. 1. (*a*) *Solve* $x^3 - 6x - 9 = 0$ *by Cardan's method.* [*B. H. 1995*]

(*b*) *Reduce the equation* $x^3 + 6x^2 - 12x + 32 = 0$ *to its standard form and then solve the equation.*

(*a*) Let $x = u^{\frac{1}{3}} + v^{\frac{1}{3}} = m + n$, where $m = u^{\frac{1}{3}}$ and $n = v^{\frac{1}{3}}$.

Then $x^3 - 3mnx - (m^3 + n^3) = 0$.

Comparing this equation with the given equation, we get

$$-3mn = -6 \text{ so that } mn = 2 \quad \ldots \quad (1)$$

and $$m^3 + n^3 = 9. \quad \ldots \quad (2)$$

Now $$(m^3 - n^3)^2 = (m^3 + n^3)^2 - 4m^3n^3 = 81 - 32 = 49$$

or, $$m^3 - n^3 = \pm 7. \quad \ldots \quad (3)$$

Adding (2) and (3), we get $2m^3 = 16, 2$

or, $$m^3 = 8, 1$$

or, $$m = 2,\ 2\omega,\ 2\omega^2;\ 1,\ \omega,\ \omega^2,$$

where ω is an imaginary cube root of unity.

From (1),

$$n = \frac{2}{m} = \frac{2}{2}, \frac{2}{2\omega}, \frac{2}{2\omega^2}; \frac{2}{1}, \frac{2}{\omega}, \frac{2}{\omega^2} = 1, \omega^2, \omega;\ 2, 2\omega^2, 2\omega\ .$$

Therefore $x = m + n = 2 + 1,\ 2\omega + \omega^2,\ 2\omega^2 + \omega$

$$= 3, 2 \cdot \tfrac{1}{2}(-1 + \sqrt{3}i) + \tfrac{1}{2}(-1 - \sqrt{3}i), 2 \cdot \tfrac{1}{2}(-1 - \sqrt{3}i) + \tfrac{1}{2}(-1 + \sqrt{3}i)$$

$$= 3, -\tfrac{3}{2} \pm \tfrac{1}{2}\sqrt{3}i.$$

(*b*) To reduce the equation to standard form, we put $x = y + h$.

Then the equation becomes

$$(y + h)^3 + 6(y + h)^2 - 12(y + h) + 32 = 0$$

or, $$y^3 + 3(h + 2)y^2 + 3(h^2 + 4h - 4)y + (h^3 + 6h^2 - 12h + 32) = 0.$$

To remove the second term, we put $h + 2 = 0$, that is, $h = -2$ and we get the standard form of the given equation as

$$y^3 - 24y + 72 = 0. \quad \ldots \quad (1)$$

Comparing this equation with the standard cubic equation

$$z^3 + 3Hz + G = 0,$$

we get $H = -8$ and $G = 72$.

Thus $(G^2 + 4H^3)$ being positive, we can apply Cardan's method for its solution.

Assume $y = u^{\frac{1}{3}} + v^{\frac{1}{3}} = m + n$, where $m = u^{\frac{1}{3}}$ and $n = v^{\frac{1}{3}}$.

Therefore $y^3 - 3mny - (m^3 + n^3) = 0.$ ... (2)

Comparing (1) and (2), we get

$$mn = 8 \text{ so that } m^3n^3 = 512 \text{ and } m^3 + n^3 = -72.$$

Thus m^3 and n^3 are the roots of the equation $t^2 + 72t + 512 = 0$,

that is, $(t + 64)(t + 8) = 0$, giving $t = -64$ and -8.

Let $m^3 = -64$ and $n^3 = -8$.

The three values of m and n are respectively

$$-4, -4\omega, -4\omega^2 \text{ and } -2, -2\omega, -2\omega^2.$$

Hence the admissible combinations are, since $mn = 8$,

$$(-4, -2), (-4\omega, -2\omega^2) \text{ and } (-4\omega^2, -2\omega).$$

Thus the values of y as given by $(m + n)$ are

$$-6, -4\omega - 2\omega^2, -4\omega^2 - 2\omega.$$

Hence the roots of the given equation are, since $x = y - 2$,

$$-6 - 2, -4\omega - 2\omega^2 - 2, -4\omega^2 - 2\omega - 2,$$

that is, $-8, -2\omega, -2\omega^2$.

Ex. 2. *Show that* $2 \sin 10^\circ$, $2 \sin 50^\circ$ *and* $(-2 \sin 70^\circ)$ *are the roots of the equation* $x^3 - 3x + 1 = 0$. [*B. H. 1964*]

Let us put $x = m + n$,

so that $x^3 - 3mnx - (m^3 + n^3) = 0.$

Comparing this equation with the given equation, we get

$$-3mn = -3, \text{ so that } m^3n^3 = 1 \text{ and } m^3 + n^3 = -1.$$

Therefore m^3 and n^3 are the roots of the equation $t^2 + t + 1 = 0$, giving

$$t = \tfrac{1}{2}(-1 \pm \sqrt{3}i).$$

Let $m^3 = -\frac{1}{2} + \frac{1}{2}\sqrt{3}i = a + ib$ and $n^3 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}i = a - ib$,

where $a = -\frac{1}{2}$ and $b = \frac{1}{2}\sqrt{3}$.

Thus $m^3 = r(\cos\theta + i \sin\theta)$ and $n^3 = r(\cos\theta - i \sin\theta)$,

where $r = \sqrt{a^2 + b^2} = \sqrt{\frac{1}{4} + \frac{3}{4}} = 1$ and $\tan\theta = -\sqrt{3}$, giving $\theta = \frac{2}{3}\pi$.

Hence the values of m and n are

$$\cos \tfrac{1}{3}(\tfrac{2}{3}\pi + 2k\pi) + i \sin \tfrac{1}{3}(\tfrac{2}{3}\pi + 2k\pi)$$

and $$\cos \tfrac{1}{3}(\tfrac{2}{3}\pi + 2k\pi) - i \sin \tfrac{1}{3}(\tfrac{2}{3}\pi + 2k\pi),$$

where k is zero or an integer.

Therefore $x = m + n = 2 \cos \tfrac{1}{3}(\tfrac{2}{3}\pi + 2k\pi)$.

Putting $k = 0$, 1 and 2, we get the three distinct roots as

$$2 \cos \tfrac{2}{9}\pi,\ 2 \cos \tfrac{8}{9}\pi,\ 2 \cos \tfrac{14}{9}\pi,$$

that is, $2 \cos 40^\circ,\ 2 \cos 160^\circ,\ 2 \cos 280^\circ,$

that is, $2 \sin 50^\circ,\ -2 \sin 70^\circ,\ 2 \sin 10^\circ.$

Examples V(A)

Transform the following equations to standard form :

1. $x^3 - 6x^2 + 4x - 7 = 0.$
2. $x^3 - 6x^2 + 10x - 3 = 0.$
3. $x^3 - 3x^2 + 12x + 16 = 0.$

Solve the following equations by Cardan's method :

4. $x^3 - 30x + 133 = 0.$ [*B. H. 1985 ; N. B. H. 1987*]
5. $x^3 - 3x^2 + 12x + 16 = 0.$
6. $x^3 - 18x - 35 = 0.$ [*B. H. 1996*]
7. $x^3 - 12x + 65 = 0.$
8. $x^3 + 12x - 12 = 0.$
9. $x^3 + 72x - 1720 = 0.$
10. $x^3 - 9x + 28 = 0.$ [*C. H. 1978*]
11. $28x^3 - 9x^2 + 1 = 0.$
12. $x^3 + 30x - 117 = 0.$
13. $x^3 + 3x^2 + 6x + 4 = 0.$
14. $x^3 - 15x - 126 = 0.$ [*T. H. 1989*]
15. $x^3 - 6x^2 + 30x - 25 = 0.$

16. Determine the roots of the equation $x^3 - 12x + 8 = 0$ in terms of trigonometric functions.

17. (*a*) Prove that the roots of the equation $x^3 - 6x - 4 = 0$ are

$$-2,\ 2\sqrt{2}\cos\tfrac{1}{12}\pi,\ 2\sqrt{2}\cos\tfrac{7}{12}\pi.$$

(*b*) Show that the roots of the equation $x^3 - 3x^2 + 3 = 0$ are

$$(1 - 2\cos\tfrac{1}{9}\pi),\ (1 - 2\cos\tfrac{5}{9}\pi),\ (1 - 2\cos\tfrac{7}{9}\pi).$$

18. Using the identity

$$x^3 + a^3 + b^3 - 3abx = (x + a + b)(x + a\omega + b\omega^2)(x + a\omega^2 + b\omega),$$

solve the equation $x^3 - 6x + 9 = 0$.

19. Find the relation between q and r in order that the equation $x^3 + qx + r = 0$ may be put into the form

$$x^4 = (x^2 + ax + b)^2.$$

Hence solve the equation $8x^3 - 36x + 27 = 0$. [*B. H. 1973*]

20. Solve the equation $2x^3 + 3x^2 + 3x + 1 = 0$.

Answers

1. $y^3 - 8y - 15 = 0$. **2.** $y^3 - 2y + 1 = 0$. **3.** $y^3 + 9y + 26 = 0$.

4. $-7, \frac{7}{2} \pm \frac{3}{2}\sqrt{3}i$. **5.** $-1, 2(1 \pm \sqrt{3}i)$.

6. $5, -\frac{5}{2} \pm \frac{1}{2}\sqrt{3}i$. **7.** $-5, \frac{5}{2} \pm \frac{3}{2}\sqrt{3}i$.

8. $2\sqrt[3]{2} - \sqrt[3]{4},\ 2\sqrt[3]{2}\omega - \sqrt[3]{4}\omega^2,\ 2\sqrt[3]{2}\omega^2 - \sqrt[3]{4}\omega$.

9. $10, -5 \pm 7\sqrt{3}i$. **10.** $-4, 2 \pm \sqrt{3}i$. **11.** $-\frac{1}{4}, \frac{1}{7}(2 \pm \sqrt{3}i)$.

12. $3, -\frac{3}{2} \pm \frac{7}{2}\sqrt{3}i$. **13.** $-1, -1 \pm \sqrt{3}i$.

14. $6, -3 \pm 2\sqrt{3}i$. **15.** $1, \frac{3}{2} \pm \frac{5}{2}\sqrt{3}i$.

16. $4\cos\frac{2}{9}\pi,\ 4\cos\frac{4}{9}\pi,\ 4\cos\frac{8}{9}\pi$. **18.** $-3, 1 - \omega, 1 - \omega^2$.

19. $q^3 + 8r^2 = 0$; $\frac{3}{2}, \frac{3}{4}(-1 \pm \sqrt{5})$. **20.** $-\frac{1}{2}, \frac{1}{2}(-1 \pm \sqrt{3}i)$.

5.6. Standard form of a biquadratic.

Let the general biquadratic equation with binomial coefficients be

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0,\ a \neq 0. \quad \ldots (1)$$

To transform this equation into one, wanting the second term, we diminish the roots of the equation (1) by h, that is, by putting $x = y + h$ and equating the coefficient of y^3 in the transformed equation to zero. This gives $h = -\frac{b}{a}$. With this choice of h, we get the transformed equation as

$$a^4y^4 + 6a^2(ac - b^2)y^2 + 4a(a^2d - 3abc + 2b^3)y + (a^3e - 4a^2bd + 6ab^2c - 3b^4) = 0.$$

Let $H = ac - b^2$, $G = a^2d - 3abc + 2b^3$ and $I = ae - 4bd + 3c^2$.

Then we can write

$$\begin{aligned} &a^3e - 4a^2bd + 6ab^2c - 3b^4 \\ &= a^2(ae - 4bd + 3c^2) - 3(a^2c^2 - 2ab^2c + b^4) \\ &= a^2I - 3(ac - b^2)^2 = a^2I - 3H^2. \end{aligned}$$

Thus the equation can be put as

$$y^4 + 6H\frac{y^2}{a^2} + 4G\frac{y}{a^3} + \frac{1}{a^4}(a^2I - 3H^2) = 0.$$

The roots of this equation are then multiplied by a and writing $z = ay$, we get

$$z^4 + 6Hz^2 + 4Gz + (a^2I - 3H^2) = 0. \quad \ldots \quad (2)$$

This equation is called the *standard form* of the biquadratic.

If $\alpha, \beta, \gamma, \delta$ be the roots of (1), then those of (2) are

$$(a\alpha + b), (a\beta + b), (a\gamma + b), (a\delta + b).$$

5.7. Euler's solution of a biquadratic.

To solve the biquadratic equation

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0, \quad \ldots \quad (1)$$

we reduce this to the standard form

$$z^4 + 6Hz^2 + 4Gz + (a^2I - 3H^2) = 0, \quad \ldots \quad (2)$$

where $H = ac - b^2$, $G = a^2d - 3abc + 2b^3$, $I = ae - 4bd + 3c^2$

To solve this equation in z, let us assume

$$z = \sqrt{p} + \sqrt{q} + \sqrt{r}. \quad \ldots \quad (3)$$

Squaring both sides of (3), we get

$$z^2 = p+q+r+2(\sqrt{pq}+\sqrt{qr}+\sqrt{rp})$$

or, $$z^2-(p+q+r)=2(\sqrt{pq}+\sqrt{qr}+\sqrt{rp}).$$

Squaring both sides again, we get

$$z^4-2(p+q+r)z^2+(p+q+r)^2$$
$$=4(pq+qr+rp)+8\sqrt{pqr}(\sqrt{p}+\sqrt{q}+\sqrt{r}).$$

By (3), we can write

$$z^4-2(p+q+r)z^2-8\sqrt{pqr}z+(p+q+r)^2$$
$$-4(pq+qr+rp)=0. \quad \ldots (4)$$

Comparing equations (2) and (4), we have

$$p+q+r=-3H,\ \sqrt{pqr}=-\tfrac{1}{2}G$$

and $(p+q+r)^2-4(pq+qr+rp)=a^2I-3H^2.$

Therefore $4(pq+qr+rp)=9H^2-a^2I+3H^2=12H^2-a^2I$

or, $$pq+qr+rp=3H^2-\tfrac{1}{4}a^2I.$$

Thus p, q, r are the roots of the equation

$$t^3+3Ht^2+(3H^2-\tfrac{1}{4}a^2I)t-\tfrac{1}{4}G^2=0. \quad \ldots (5)$$

This is known as *Euler's cubic.*

Now it is seen that $G^2+4H^3=a^2(HI-aJ),$ $\ldots$ (6)

where $J=ace+2bcd-ad^2-eb^2-c^3.$

Thus $-\tfrac{1}{4}G^2=H^3-\tfrac{1}{4}a^2HI+\tfrac{1}{4}a^3J$ and (5) becomes

$$t^3+3Ht^2+(3H^2-\tfrac{1}{4}a^2I)t+(H^3-\tfrac{1}{4}a^2HI+\tfrac{1}{4}a^3J)=0$$

or, $$4(t+H)^3-a^2I(t+H)+a^3J=0.$$

Putting $t+H=a^2\theta$, this equation reduces to

$$4a^3\theta^3-Ia\theta+J=0, \quad \ldots (7)$$

which is known as the *reducing cubic* of the biquadratic.

The equation (1) is thus solved by establishing relations between the roots of this reducing cubic with those of the biquadratic.

Now, since $t+H=a^2\theta$, therefore $t=a^2\theta-H=a^2\theta-ac+b^2$. If $\theta_1, \theta_2, \theta_3$ be the roots of the reducing cubic, then the corresponding roots of the Euler's cubic (5) are given by

$$p=b^2-ac+a^2\theta_1,\ q=b^2-ac+a^2\theta_2,\ r=b^2-ac+a^2\theta_3.$$

Then, by (3),

$$z = \sqrt{b^2 - ac + a^2\theta_1} + \sqrt{b^2 - ac + a^2\theta_2} + \sqrt{b^2 - ac + a^2\theta_3} \quad \ldots \quad (8)$$

Now the values of z as obtained from (8) are eight in number, if we consider the ambiguity of sign ($\pm$) associated with each radical. But there should be only four values of z. To get a proper selection of signs, we should utilise the condition $\sqrt{pqr} = -\frac{1}{2}G$,

that is, $$\sqrt{r} = -\frac{G}{2\sqrt{pq}}.$$

Thus $$z = \sqrt{p} + \sqrt{q} - \frac{G}{2\sqrt{pq}}. \quad \ldots \quad (9)$$

If we now consider the double signs for both the radicals $\sqrt{p}$ and $\sqrt{q}$, then we get only four values of z by all possible combinations of these double signs. Thus, for the roots of equation (1), we can write

$$ax + b = z = \sqrt{p} + \sqrt{q} - \frac{G}{2\sqrt{pq}}$$

$$= \sqrt{b^2 - ac + a^2\theta_1} + \sqrt{b^2 - ac + a^2\theta_2} - \frac{G}{2\sqrt{b^2 - ac + a^2\theta_1}\ \sqrt{b^2 - ac + a^2\theta_2}},$$

where θ_1 and θ_2 are any two roots of the reducing cubic (7).

5.8. Descartes' method.

The given biquadratic equation is first reduced to the standard form

$$z^4 + 6Hz^2 + 4Gz + (a^2I - 3H^2) = 0. \quad \ldots \quad (1)$$

Let this equation be supposed to be represented by

$$(z^2 + Mz + N)(z^2 - Mz + K) = 0. \quad \ldots \quad (2)$$

Comparing (1) and (2), we get

$$6H = K + N - M^2,\ 4G = M(K - N),\ a^2I - 3H^2 = NK.$$

From the first two relations, we get

$$2K = 6H + M^2 + \frac{4G}{M} \quad \text{and} \quad 2N = 6H + M^2 - \frac{4G}{M}.$$

Substituting these values of K and N in the third relation, we get

$$M^6 + 12HM^4 - 4(a^2I - 12H^2)M^2 - 16G^2 = 0,$$

which is a cubic in M^2 and can easily be solved to get the values of M^2. This, in turn, determines the corresponding values of K and N. Thus we are led to the solution of two quadratic equations

$$z^2 + Mz + N = 0 \text{ and } z^2 - Mz + K = 0.$$

Solutions of these quadratic equations will be the solutions of (1).

5.9. Ferrari's method.

(*a*) Let the biquadratic equation

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0 \quad \ldots (1)$$

be multiplied by a and put in the following form :

$$(ax^2 + 2bx + c + 2a\theta)^2 - (2Mx + N)^2 = 0, \quad \ldots (2)$$

where M, N, θ are to be determined.

Comparing the coefficients of like powers of x in (1) and (2), we get

$$M^2 = b^2 - ac + a^2\theta, \; N^2 = (c + 2a\theta)^2 - ae,$$

$$MN = bc - ad + 2ab\theta. \quad \ldots (3)$$

Thus

$$(bc - ad + 2ab\theta)^2 = (MN)^2 = (b^2 - ac + a^2\theta)\{(c + 2a\theta)^2 - ae\}$$

or, $4a^3\theta^3 - (ae - 4bd + 3c^2)a\theta + (ace + 2bcd - ad^2 - b^2e - c^3) = 0$

or, $4a^3\theta^3 - Ia\theta + J = 0, \quad \ldots (4)$

which is the reducing cubic of Euler's method. Values of θ as obtained from (4) when substituted in (3) will determine M and N.

Then, solving the two quadratic equations as given by (2), we get the solution of the equation (1).

(*b*) Let the biquadratic equation be

$$x^4 + bx^3 + cx^2 + dx + e = 0.$$

Then $x^4 + bx^3 + \frac{1}{4}b^2x^2 = \frac{1}{4}b^2x^2 - cx^2 - dx - e$

or, $(x^2 + \frac{1}{2}bx)^2 = (\frac{1}{4}b^2 - c)x^2 - dx - e.$

The basic idea in Ferrari's method is to make the right hand side a perfect square. For this purpose, $\{y(x^2+\frac{1}{2}bx)+\frac{1}{4}y^2\}$ is added to both sides ; then we get

$$(x^2+\tfrac{1}{2}bx+\tfrac{1}{2}y)^2=(y+\tfrac{1}{4}b^2-c)x^2+(\tfrac{1}{2}by-d)x+(\tfrac{1}{4}y^2-e).$$

We choose y in such a manner that the right hand side becomes a perfect square. So y is given by

$$(\tfrac{1}{2}by-d)^2=4(y+\tfrac{1}{4}b^2-c)(\tfrac{1}{4}y^2-e)$$

or, $$y^3-cy^2+(bd-4e)y+(4ce-b^2e-d^2)=0.$$

This is the reducing cubic for the given biquadratic. For a value of y given by this equation, the given biquadratic may be written in the form

$$(x^2+\tfrac{1}{2}bx+\tfrac{1}{2}y)^2=(px+q)^2$$

or, $$x^2+\tfrac{1}{2}bx+\tfrac{1}{2}y=\pm(px+q)$$

and hence the solution of the given equation may be obtained, by solving these quadratic equations.

Any one value of y will give the solution of the equation.

5.10. Illustrative Examples.

Ex. 1. *Solve the equation* $x^4-2x^2+8x-3=0$. [*B. H. 1965*]

Let $x=\sqrt{p}+\sqrt{q}+\sqrt{r}$.

Squaring and transposing, we get

$$x^2-(p+q+r)=2(\sqrt{qr}+\sqrt{rp}+\sqrt{pq}).$$

Squaring again, we get

$$x^4-2(p+q+r)x^2-8x\sqrt{pqr}+(p+q+r)^2-4(qr+rp+pq)=0.$$

Comparing this equation with the given equation, we have

$$p+q+r=1,\ \sqrt{pqr}=-1$$

and $$(p+q+r)^2-4(qr+rp+pq)=-3.$$

Therefore $$qr+rp+pq=1.$$

Thus p, q, r are the roots of the Euler's cubic $t^3-t^2+t-1=0$, giving $t=1$ and $\pm i$.

Hence $p=1,\ q=i,\ r=-i,$

so that $$\sqrt{p}=\pm 1,\ \sqrt{q}=\pm\frac{1+i}{\sqrt{2}},\ \sqrt{r}=\pm\frac{1-i}{\sqrt{2}}.$$

But $\sqrt{pqr}=-1$, a negative quantity.

Hence $x = -1 + \frac{1}{\sqrt{2}}(1+i) + \frac{1}{\sqrt{2}}(1-i),\ -1 - \frac{1}{\sqrt{2}}(1+i) - \frac{1}{\sqrt{2}}(1-i),$

$$1 + \frac{1}{\sqrt{2}}(1+i) - \frac{1}{\sqrt{2}}(1-i),\ 1 - \frac{1}{\sqrt{2}}(1+i) + \frac{1}{\sqrt{2}}(1-i).$$

Thus the roots are $-1 \pm \sqrt{2},\ 1 \pm \sqrt{2}i.$

Ex. 2. *Reduce the biquadratic* $x^4 + 6x^3 + 14x^2 + 22x + 5 = 0$ *to its standard form. Then solve the equation.*

To remove the second term, we put $x = y + h$. Then the given equation becomes

$$(y+h)^4 + 6(y+h)^3 + 14(y+h)^2 + 22(y+h) + 5 = 0.$$

The coefficient of y^3 in this equation is $(4h + 6)$. To remove the second term, we are to put $4h + 6 = 0$, that is, $h = -\frac{3}{2}$.

In order to reduce the biquadratic to the standard form, we are to multiply the roots of the equation by 2, then the roots are to be increased by 3. Thus putting $y = 2x$, the equation becomes

$$y^4 + 2.6y^3 + 4.14y^2 + 8.22y + 16.5 = 0$$

or, $\quad y^4 + 12y^3 + 56y^2 + 176y + 80 = 0.$

Increasing the roots by 3, we get the standard form of the given equation as

$$z^4 + 2z^2 + 56z - 187 = 0. \qquad \ldots \quad (1)$$

Let us solve this equation by Descartes' method. For that, let us put (1) as

$$(z^2 + Mz + N)(z^2 - Mz + K) = 0. \qquad \ldots \quad (2)$$

Comparing (1) and (2), we get

$$K + N - M^2 = 2,\ M(K - N) = 56,\ KN = -187.$$

Therefore $\quad K + N = 2 + M^2,\ K - N = \frac{56}{M}.$

Hence $(2 + M^2)^2 - \left(\frac{56}{M}\right)^2 = (K+N)^2 - (K-N)^2 = 4KN$

$$= -187 \times 4 = -748.$$

Putting $M^2 = t$, we get $(t+2)^2 - \frac{3136}{t} = -748$

or, $\quad t^3 + 4t^2 + 752t - 3136 = 0.$

By trial, we get $t = 4$. Hence $M^2 = 4$, that is, $M = 2$.

Thus $K + N = 6,\ K - N = 28$, giving $K = 17$ and $N = -11$.

Hence (2) becomes $(z^2 + 2z - 11)(z^2 - 2z + 17) = 0.$

Therefore $\quad z = -1 \pm 2\sqrt{3}, 1 \pm 4i.$

Again $y = z - 3 = -4 \pm 2\sqrt{3}, -2 \pm 4i.$

Therefore $x = \frac{1}{2}y = -2 \pm \sqrt{3}, -1 \pm 2i.$

Ex. 3. *Solve the biquadratic equation*

$$x^4 + 5x^3 + x^2 - 13x + 6 = 0. \qquad [C.\ H.\ 1962]$$

Here $nah + b = 0$ gives $h = -\frac{5}{4}$. Thus to reduce this equation to the standard form, we are to multiply the roots by 4, putting $x = \frac{1}{4}y$; then increase the roots by 5, putting $y = z - 5$.

The first transformed equation is thus

$$y^4 + 20y^3 + 16y^2 - 832y + 1536 = 0. \qquad \ldots \quad (1)$$

Increasing the roots by 5, we get the standard form of the given equation as

$$z^4 - 134z^2 + 8z + 4221 = 0. \qquad \ldots \quad (2)$$

Let us put the equation in the form

$$(z^2 + Mz + N)(z^2 - Mz + K) = 0. \qquad \ldots \quad (3)$$

Comparing (2) and (3), we get

$$K + N - M^2 = -134,\ M(K - N) = 8,\ NK = 4221.$$

Therefore $K + N = M^2 - 134$ and $K - N = \frac{8}{M}$.

Hence $$(M^2 - 134)^2 - \left(\frac{8}{M}\right)^2 = 4 \times 4221.$$

Putting $t = M^2$, this becomes $(t - 134)^2 - \frac{64}{t} = 16884$

or, $$t^3 - 268t^2 + 1072t - 64 = 0.$$

By trial, we get $t = 4$. Hence $M^2 = 4$ and $M = 2$.

Thus $K + N = -130$ and $K - N = 4$, giving $K = -63$ and $N = -67$.

Then equation (3) becomes $(z^2 + 2z - 67)(z^2 - 2z - 63) = 0$

or, $$z = 9, -7, -1 \pm \sqrt{68}.$$

Therefore $y = z - 5 = 4, -12, -6 \pm 2\sqrt{17}$.

Hence $x = \frac{1}{4}y = 1, -3, \frac{1}{2}(-3 \pm \sqrt{17})$.

Ex. 4. *Solve, by Ferrari's method,* $x^4 + 12x = 5$.

[K. H. 1979 ; C. H. 1985 ; N. B. H. 1985 ; V. H. 1989 ; B. H. 1994]

We have $$x^4 + 12x - 5 = 0 \qquad \ldots \quad (1)$$

or, $$(x^2)^2 = -12x + 5.$$

Adding $(x^2y + \frac{1}{4}y^2)$ to both sides, we get

$$(x^2 + \tfrac{1}{2}y)^2 = x^2y - 12x + (\tfrac{1}{4}y^2 + 5). \quad \ldots \quad (2)$$

Now y is so chosen that the right hand side becomes a perfect square.

So we take $(-12)^2 = 4y(\frac{1}{4}y^2 + 5)$

or, $y^3 + 20y - 144 = 0$

or, $(y-4)(y^2 + 4y + 36) = 0.$

Thus one value of y is 4.

Hence, from (2), the equation (1) may be written as

$$(x^2+2)^2 = 4x^2 - 12x + 9 = (2x-3)^2$$

or, $x^2 + 2 = \pm(2x - 3)$

or, $x^2 - 2x + 5 = 0, x^2 + 2x - 1 = 0.$

Therefore $x = 1 \pm 2i, -1 \pm \sqrt{2}.$

Examples V(B)

Solve the following equations :

1. $x^4 - 3x^3 + 5x^2 - 5x + 2 = 0.$
2. $x^4 - 4x^2 - 3x + 6 = 0.$
3. $x^4 + 5x^2 + 2x + 8 = 0.$
4. $x^4 + 2x^3 + 14x + 15 = 0.$
5. $4x^4 - 16x^3 + 21x^2 - 13x + 6 = 0.$
6. $x^4 + 2x^3 - 7x^2 - 8x + 12 = 0.$
7. $2x^4 + 5x^3 - 8x^2 - 17x - 6 = 0.$
8. $x^4 - 2x^3 - 9x^2 + 6x + 9 = 0.$
9. $x^4 - x^3 + 2x^2 + x + 3 = 0.$
10. $x^4 - 6x^2 + 16x - 15 = 0.$
11. $x^4 - 4x^3 + 16x^2 + 48x - 336 = 0.$
12. $x^4 - 4x^3 + 5x + 2 = 0.$ [*B. H. 1961*]
13. $x^4 + 20x^3 + 143x^2 + 430x + 462 = 0.$ [*B. H. 1962*]
14. $x^4 - 3x^2 - 6x - 2 = 0.$ [*A. H. 1966 ; N. B. H. 1988*]
15. $x^4 - 2x^2 + 8x - 3 = 0.$ [*B. H. 1965 ; C. H. 1988 ; V. H. 1990*]
16. $x^4 + 5x^3 + x^2 - 13x + 6 = 0.$ [*C. H. 1962*]

17. Show that the reducing cubic of the biquadratic

$$x^4 - x^3 - 3x^2 + 5x - 2 = 0$$

has all its roots zero and find Euler's solutions of the biquadratic.

18. Solve, by Euler's method, the equation $x^4 + 4x^3 - 6x^2 + 20x + 8 = 0$, being given that $\theta = 2$ is a root of its reducing cubic. [*C. H. 1976; V. H. 2004*]

19. Solve, by Ferrari's method, the equations

(*i*) $x^4 - 18x^2 + 32x - 15 = 0$. [*C. H. 1987; T. H. 2008*]

(*ii*) $x^4 - 2x^3 - 5x^2 + 10x - 3 = 0$. [*V. H. 1987 ; B. H. 1992*]

(*iii*) $x^4 - 9x^3 + 28x^2 - 38x + 24 = 0$. [*C. H. 1984*]

(*iv*) $x^4 + 3x^3 + x^2 - 2 = 0$. [*B. H. 1989, 1997*]

20. (*a*) If $f(x) = x^4 + 6x^3 + 14x^2 + 22x + 5$, then find α, β and λ, so that $f(x)$ can be expressed in the form $(x^2 + 3x + \lambda)^2 - (\alpha x + \beta)^2$.

Hence find all the roots of the equation $f(x) = 0$. [*C. H. 1982*]

(*b*) Express $f(x) = x^4 - 2x^3 - 5x^2 + 10x - 3$ in the form

$$(x^2 + px + q)^2 - (ax + b)^2$$

and hence solve the equation $f(x) = 0$. [*C. H. 1980*]

(*c*) Express the equation $x^4 - 6x^2 - 16x - 15 = 0$ in the form $(x^2 + \lambda)^2 - (mx + n)^2 = 0$. Hence solve the equation. [*C. H. 1997*]

(*d*) Prove that the condition that the biquadratic $a_0x^4 + 4a_1x^3 + 6a_2x^2 + 4a_3x + a_4 = 0$ may be in the form $\lambda(x^2 + 2px + q)^2 + \mu(x^2 + 2px + q) + \nu = 0$ is $a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3 = 0$. [*V. H. 2007*]

Answers

1. $1, 1, \frac{1}{2}(1 \pm \sqrt{7}i)$.
2. $1, 2, \frac{1}{2}(-3 \pm \sqrt{3}i)$.
3. $\frac{1}{2}(1 \pm \sqrt{15}i), \frac{1}{2}(-1 \pm \sqrt{7}i)$.
4. $-1, -3, 1 \pm 2i$.
5. $2, \frac{3}{2}, \frac{1}{4}(1 \pm \sqrt{7}i)$.
6. $1, 2, -2, -3$.
7. $-3, -1, -\frac{1}{2}, 2$.
8. $\frac{1}{2}(-1 \pm \sqrt{13}), \frac{1}{2}(3 \pm \sqrt{21})$.
9. $\frac{1}{2}(-1 \pm \sqrt{3}i), 1 \pm \sqrt{2}i$.
10. $-1 \pm \sqrt{6}, 1 \pm \sqrt{2}i$.
11. $\pm 2\sqrt{3}, 2 \pm 2\sqrt{6}i$.
12. $\frac{1}{2}(1 \pm \sqrt{5}), \frac{1}{2}(3 \pm \sqrt{17})$.
13. $-5 \pm \sqrt{3}, -7, -3$.
14. $-1 \pm i, 1 \pm \sqrt{2}$.
15. $-1 \pm \sqrt{2}, 1 \pm \sqrt{2}i$.
16. $1, -3, \frac{1}{2}(-3 \pm \sqrt{17})$.

17. $1,1,1,-2$.

18. $1\pm\sqrt{3}\,i,-3\pm\sqrt{7}$.

19. (*i*) $1,1,3,-5$.

(*ii*) $\frac{1}{2}\left(-1\pm\sqrt{13}\right),\frac{1}{2}\left(3\pm\sqrt{5}\right)$.

(*iii*) $3,4,1\pm i$.

(*iv*) $-1\pm\sqrt{3},\frac{1}{2}\left(-1\pm\sqrt{3}\,i\right)$.

20. (*a*) $\alpha=1,\ \beta=-2,\ \lambda=3;\ -1\pm2i,-2\pm\sqrt{3}$.

(*b*) $\left(x^2-x-1\right)^2-(2x-2)^2;\ \frac{1}{2}\left(-1\pm\sqrt{13}\right),\ \frac{1}{2}\left(1\pm\sqrt{5}\right)$.

(*c*) $\left(x^2-1\right)^2=(2x+4)^2;\ 1\pm\sqrt{6},-1\pm\sqrt{2}\,i$.

5.11. Limits of the roots of equations.

To find the real roots of numerical equations, we want to narrow the region within which they lie. Any positive number which is greater than the greatest of the positive roots of an equation is called a *superior* or *upper limit of the positive roots* of the equation. Any positive number which is smaller than the smallest of the positive roots of an equation is called an *inferior* or *lower limit of the positive roots*. We search for smaller superior limits and greater inferior limits.

A *superior limit of the negative roots* of an equation is a negative number which is greater than the greatest of them and an *inferior limit of the negative roots* is a negative number which is smaller than the smallest of them.

To find superior limits of the positive roots of an equation, we generally use the following three propositions :

(*a*) *If, in the equation*

$$x^n+p_1x^{n-1}+p_2x^{n-2}+\cdots\cdots+p_{n-1}x+p_n=0,$$

the $(r+1)$*-th term be the first negative term and if* $(-p_s)$ *be the greatest negative coefficient, then* $\left(\sqrt[r]{p_s}+1\right)$ *is a superior limit of the positive roots of the equation.*

Let $f(x)=x^n+p_1x^{n-1}+p_2x^{n-2}+\cdots\cdots+p_{n-1}x+p_n$.

$f(x)$ is positive for any value of x which makes

$$x^n>p_s\left(x^{n-r}+x^{n-r-1}+\cdots\cdots+x+1\right),$$

that is, $x^n>p_s\dfrac{x^{n-r+1}-1}{x-1}$,

that is, $x^{n+1}-x^n>p_s\left(x^{n-r+1}-1\right)$, when $x>1$.

This inequality is satisfied, if $x^{n+1} - x^n > p_s x^{n-r+1}$,

that is, if $x^r - x^{r-1} > p_s$,

that is, if $x^{r-1}(x-1) > p_s$.

Since $x^{r-1} > (x-1)^{r-1}$, this inequality is satisfied,

if $(x-1)^r \geq p_s$,

that is, if $x - 1 \geq \sqrt[r]{p_s}$,

that is, if $x \geq \sqrt[r]{p_s} + 1$.

(b) If, in the equation $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \cdots\cdots + a_{n-1}x + a_n = 0$, *each negative coefficient be taken positively and divided by the sum of all the positive coefficients which precede it, then the greatest quotient thus formed increased by unity is a superior limit of the positive roots of the equation.*

(c) Any number h, which makes $f(x)$ *and all its derivatives* $f'(x), f''(x), f'''(x), \ldots\ldots$ *positive, is a superior limit of the positive roots of the equation* $f(x) = 0$.

This method is due to *Newton*.

To prove this, we diminish the roots of the equation $f(x) = 0$ by h.

Then, taking $y = x - h$, we get the transformed equation as

$$f(y+h) = f(h) + f'(h)y + \frac{f''(h)}{2!}y^2 + \frac{f'''(h)}{3!}y^3 + \cdots\cdots + \frac{f^n(h)}{n!}y^n = 0.$$

If h be such that $f(h), f'(h), f''(h), \ldots\ldots, f^n(h)$ are all positive, then this equation in y can not have a positive root and consequently the equation $f(x) = 0$ has no root greater than h.

Hence h is a superior limit of the positive roots of the equation

$$f(x) = 0.$$

Although this method is very laborious, it always gives very close limits.

If all the roots of the equation be real, then the limit obtained by this method is the next integer above the greatest positive root.

Sometimes we can find a suitable superior limit by merely grouping the terms of the equation.

To find an inferior limit of the positive roots of a given equation $f(x)=0$, we first find a superior limit l of the positive roots of the equation $f\left(\frac{1}{x}\right)=0$. Then $\frac{1}{l}$ is an inferior limit of the positive roots of the given equation.

To find limits of the negative roots of a given equation $f(x)=0$, we are to find limits of the positive roots of the equation $f(-x)=0$.

If l and l' be superior and inferior limits of the positive roots of the equation $f(-x)=0$, then $(-l)$ and $(-l')$ are the limits of the negative roots of the equation $f(x)=0$.

5.12. Separation of the roots of equations.

To separate the roots of equations, we have earlier discussed some rules, like Rolle's theorem, Descartes' rule of signs. Here we discuss some more rules for this purpose.

First we discuss Fourier's theorem, which was later modified by Budan. This is very convenient to apply but it may fail sometimes. Then we discuss Sturm's theorem, which is laborious, but is unfailing in its application.

To prove Fourier's theorem, we require two subsidiary theorems.

5.13. Two subsidiary theorems.

Theorem 1. *If α be a root of the equation $f(x)=0$, then, as the variable x passes from $(\alpha-h)$ to $(\alpha+h)$, h being a small positive quantity, the functions $f(x)$ and $f'(x)$ have opposite signs just before $x=\alpha$ and the same sign just after $x=\alpha$.*

Here $f(\alpha)=0$ and by Taylor's expansion, we have

$$f(\alpha+h)=hf'(\alpha)+\frac{h^2}{2!}f''(\alpha)+\cdots\cdots+\frac{h^r}{r!}f^r(\alpha)+\cdots\cdots$$

and $f'(\alpha+h)=f'(\alpha)+hf''(\alpha)+\cdots\cdots+\frac{h^{r-1}}{(r-1)!}f^r(\alpha)+\cdots\cdots$

Now the signs of these expressions depend on those of their first terms. Hence $f(\alpha+h)$ and $f'(\alpha+h)$ have the same or opposite signs according as $h>$ or <0, which proves the theorem.

Cor. The theorem also holds good when α is a multiple root of any order of the equation $f(x)=0$.

Theorem 2. *If α be a multiple root of the equation $f(x)=0$ of multiplicity r, then, as the variable x passes from $(\alpha-h)$ to $(\alpha+h)$, h being a small positive quantity, the signs of the functions*

$$f(x), f'(x), f''(x), \ldots\ldots, f^r(x)$$

are alternately positive and negative or negative and positive just before $x=\alpha$ and all the functions have the same sign just after $x=\alpha$.

Here $f(\alpha)=0,\ f'(\alpha)=0,\ f''(\alpha)=0, \ldots\ldots, f^{r-1}(\alpha)=0$.

Therefore $$f(\alpha+h)=\frac{h^r}{r!}f^r(\alpha)+\frac{h^{r+1}}{(r+1)!}f^{r+1}(\alpha)+\cdots\cdots$$

$$f'(\alpha+h)=\frac{h^{r-1}}{(r-1)!}f^r(\alpha)+\frac{h^r}{r!}f^{r+1}(\alpha)+\cdots\cdots$$

$$f''(\alpha+h)=\frac{h^{r-2}}{(r-2)!}f^r(\alpha)+\frac{h^{r-1}}{(r-1)!}f^{r+1}(\alpha)+\cdots\cdots$$

.....

.....

$$f^r(\alpha+h)=f^r(\alpha)+hf^{r+1}(\alpha)+\cdots\cdots$$

Now the signs of these expressions depend on those of their first terms. Hence they have alternate signs when $h<0$ and they have the same sign when $h>0$.

5.14. Fourier's theorem.

The number of real roots of the equation $f(x)=0$ of degree n between two real numbers a and b, a being less than b, cannot be greater than the excess of the number of changes of sign in the sequence formed by $f(x)$ and its successive derivatives when a is substituted for x over the number of changes of sign when b is substituted for x. If the number of real roots be less than that difference, then it will be by an even number.

In other words, *let p be the number of real roots of the equation* $f(x)=0$ *of degree n between two real numbers a and b,* $(a<b)$. *If q and r be the number of changes of sign in the sequence formed by* $f(x)$ *and its successive derivatives, that is,*

$f(x), f'(x), f''(x), \ldots\ldots, f^{n}(x)$ *(called Fourier's functions) when* $x=a$ *and when* $x=b$ *respectively, then*

$$q \geq r,\ p \neq q-r \text{ and } \{(q-r)-p\}$$

is either an even number or zero.

In particular, if $q-r=1$, *then there is just one real root in the interval* (a,b) *and if* $q-r=0$, *then there is no real root in the interval.*

Of the two numbers a and b $(>a)$, one or both of them may be negative, which is meant that a is nearer to $(-\infty)$ than b.

We assume that x increases continually from a to b.

The following different cases may arise :

(*i*) The value of x may pass through a single root of the equation

$$f(x)=0\ .$$

(*ii*) It may pass through a multiple root of the equation $f(x)=0$ of multiplicity r.

(*iii*) It may pass through a root of the equation $f^{m}(x)=0$, not occurring in either $f^{m-1}(x)=0$ or $f^{m+1}(x)=0$.

(*iv*) It may pass through a multiple root of the equation $f^{m}(x)=0$ of multiplicity r and not occuring in $f^{m-1}(x)=0$.

Now, in the first case, if α be a single root of the equation $f(x)=0$, then only one change of sign is lost, since f and f' have unlike signs just before $x=\alpha$ and they have like signs just after $x=\alpha$.

In the second case, if α be a multiple root of the equation $f(x)=0$ of multiplicity r, then r changes of sign are lost in the sequence $f, f', f'', \ldots\ldots, f^{r}$, since they have alternate signs just before $x=\alpha$ and same sign just after $x=\alpha$.

In the third case, let x pass through a value β which makes

$$f^{m}(x)=0\ .$$

Since $f^{m-1}(\beta) \neq 0$ and $f^{m+1}(\beta) \neq 0$, therefore, in the sequence $f^{m-1}(\beta), f^{m}(\beta), f^{m+1}(\beta)$, there is no loss or gain of changes of sign when $f^{m-1}(\beta)$ and $f^{m+1}(\beta)$ have opposite signs, but two changes of sign are lost when $f^{m-1}(\beta)$ and $f^{m+1}(\beta)$ have same sign.

In the fourth case, let x pass through a multiple root β of the equation $f^{m}(x) = 0$ of multiplicity r. Then the r functions

$$f^{m}(x),\ f^{m+1}(x), \ldots\ldots, f^{m+r-1}(x)$$

all vanish for $x = \beta$ but $f^{m-1}(\beta) \neq 0$ and $f^{m+r}(\beta) \neq 0$.

If r be even, then there is a loss of r changes of sign in both the cases of opposite signs and same sign of $f^{m-1}(\beta)$ and $f^{m+r}(\beta)$. If r be odd, then there is a loss of $(r-1)$ or $(r+1)$ changes of sign according as $f^{m-1}(\beta)$ and $f^{m+r}(\beta)$ have opposite signs or same sign.

Thus, in this case, no change of sign is ever gained but if any are lost, their number is even.

It is very difficult to use this form of the theorem in practice.

Budan modified Fourier's theorem in the following form :

Let the roots of the equation $f(x) = 0$ be first diminished by a and then by b, where a and b are two real numbers, a being less than b. Also let p be the number of real roots of the equation $f(x) = 0$ between a and b. If q and r be the respective number of changes of sign in the transformed equations, then $p \not> q - r$.

Here the transformed equations are

$$f(a) + f'(a)y + \frac{f''(a)}{2!}y^2 + \cdots\cdots + \frac{f^{n}(a)}{n!}y^{n} = 0$$

and $$f(b) + f'(b)y + \frac{f''(b)}{2!}y^2 + \cdots\cdots + \frac{f^{n}(b)}{n!}y^{n} = 0.$$

The changes of sign of these two equations depend on the Fourier's functions and hence the result follows from Fourier's theorem.

This form is more convenient for practical purposes.

Cor.1. Considering the number of changes of sign lost during the passage of x from a small negative value $(-h)$ to a small positive value h, we get the following, from the fourth case of Fourier's theorem :

If m consecutive terms be absent in the equation $f(x)=0$, then, if m be even, the equation $f(x)=0$ has atleast m imaginary roots and if m be odd, there are atleast $(m+1)$ or atleast $(m-1)$ imaginary roots according as the terms between which m terms are absent have the same or opposite signs.

This is *De Gua's rule* for imaginary roots.

Cor. 2. When $x=0$, the Fourier's functions

$$f(x), f'(x), f''(x), \ldots\ldots, f^{n}(x)$$

have the same signs as those of the coefficients $a_n, a_{n-1}, a_{n-2}, \ldots\ldots, a_1, a_0$ of the proposed equation $f(x)=0$ and when $x=+\infty$, all the functions are positive. According to Fourier's theorem, the number of real roots between 0 and $(+\infty)$, that is, the number of positive roots cannot exceed the number of variations of sign lost during the passage from 0 to $(+\infty)$, that is, the number of changes of sign in the coefficients of $f(x)$. Similar rule for negative roots follows in the usual way.

This is *Descartes' rule of signs.*

Cor.3. Let a number h be found such that all the Fourier's functions $f(x), f'(x), f''(x), \ldots\ldots, f^{n}(x)$ are positive for $x=h$. Again, all of them are positive for $x=+\infty$. Then, by Fourier's theorem, there is no real root of the equation $f(x)=0$ between h and $(+\infty)$. Hence h is the superior limit of positive roots of the equation.

This is *Newton's method* to find the limits of the roots of equations.

5.15. Sturm's theorem.

Let $f(x)$ be a given polynomial and $f_1(x)$ be its first derivative. If, in the process of finding the highest common factor of $f(x)$ and $f_1(x)$, the successive remainders (with their signs changed) be $f_2(x), f_3(x), \ldots\ldots, f_m(x)$, then $f(x), f_1(x), f_2(x), \ldots\ldots, f_m(x)$ are called *Sturm's functions.*

$f_1(x), f_2(x), \ldots\ldots, f_m(x)$ are known as *auxiliary functions.*

If $q_1, q_2, \ldots\ldots, q_{m-1}$ be the successive quotients in the process of finding the highest common factor of $f(x)$ and $f_1(x)$, then

$$f(x) = q_1 f_1(x) - f_2(x),\ f_1(x) = q_2 f_2(x) - f_3(x), \ldots\ldots,$$

$$f_{m-2}(x) = q_{m-1} f_{m-1}(x) - f_m(x).$$

If $f(x) = 0$ has no multiple root, then $f(x)$ and $f_1(x)$ have no common factor and consequently the last remainder $f_m(x)$ will be independent of x while if $f(x) = 0$ has multiple roots, then the last remainders will be a polynomial in x.

Sturm's theorem states that *if $f(x)$ be a polynomial and a, b $(> a)$ be two real numbers, then the number of distinct real roots (if any multiple root exists, that is counted once only) of the equation $f(x) = 0$ between a and b is equal to the difference between the number of changes of sign in the sequence of Sturm's functions $f(x), f_1(x), f_2(x), \ldots\ldots, f_m(x)$ when a is substituted for x and that when b is substituted for x.*

Here two cases may arise.

Case I. *The equation $f(x) = 0$ has no multiple root.*

In this case, we can draw the following conclusions :

(*i*) The last Sturm's function $f_m(x)$ is numerical, that is, independent of x.

(*ii*) No two consecutive terms of the sequence of Sturm's functions can vanish for the same value of x in the interval (a, b) ; since , in that case, all the subsequent terms including $f_m(x)$ would vanish.

(*iii*) If any term of the sequence of Sturm's functions, except the first, vanishes for some x in the interval (a, b), then the terms, which precede and follow it, have opposite signs.

Thus, if $f_i(x) = 0$, then $f_{i-1}(x) = -f_{i+1}(x)$.

A similar inference arises if one of the q's be zero, that is, if $q_i = 0$, then

$$f_{i-1}(x) = -f_{i+1}(x).$$

We now suppose that x increases continuously from $x = a$ to $x = b$ and consider the signs of Sturm's functions. As x varies, no one of Sturm's functions can change its sign unless x passes through a value which makes that function vanish.

Next we suppose that x passes through a value α which makes just one of Sturm's functions vanish. If $f(\alpha)=0$, then one change of sign is lost in the sequence of Sturm's functions, since $f(x)$ and $f_1(x)$ have opposite signs just before $x=\alpha$ and they have the same sign just after $x=\alpha$. If $f_i(\alpha)=0$, where $i=1,2,.....,(m-1)$, then no change of sign is gained or lost, since $f_i(\alpha)=0$ implies that $f_{i-1}(x)=-f_{i+1}(x)$. If $i=1$, then $f_0(\alpha)$ stands for $f(\alpha)$. Since $f_{i-1}(x)$ and $f_{i+1}(x)$ are continuous at $x=\alpha$, so each of them is of invariable sign near $x=\alpha$.

Hence, just before and also just after $x=\alpha$, the signs of $f_{i-1}(x), f_i(x), f_{i+1}(x)$ are either $++-$ or $+--$ or $-++$ or $--+$, showing that no change of sign is lost or gained.

If x passes through a value α which makes more than one of Sturm's functions vanish, then no two of them will be consecutive functions. If $f(x)$ be one of them, then one change of sign is lost between $f(x)$ and $f_1(x)$ but no change of sign is gained or lost in the sequence $f_1(x), f_2(x), ..., f_n(x)$ and thus one change of sign is lost in the sequence of Sturm's functions. On the other hand, if $f(x)$ be not one of them, then no change of sign is gained or lost.

Therefore, as x increases, a change of sign in the sequence of Sturm's functions is lost only when x passes through a root of $f(x)=0$ and in all other circumstances, there is no gain or no loss of change of signs.

This proves the theorem for the case of non-multiple roots.

Case II. *The equation* $f(x)=0$ *has multiple roots.*

In this case, we suppose that

$$f(x)=(x-\alpha)^p(x-\beta)^q(x-\gamma)^r.....,$$

where $p,q,r,.....$ are positive integers and $\alpha,\beta,\gamma,.....$ are all different.

Then the H.C.F. of $f(x)$ and $f_1(x)$ is

$$(x-\alpha)^{p-1}(x-\beta)^{q-1}(x-\gamma)^{r-1}..... = F \text{ (say)}.$$

Therefore all the Sturm's functions are divisible by F.

If $\phi(x), \phi_1(x), \phi_2(x), \ldots\ldots, \phi_m(x)$ be the quotients in the division of Sturm's functions by F, then $\phi(x) = (x-\alpha)(x-\beta)(x-\gamma)\ldots\ldots$

and $\phi_m(x)$ is independent of x.

Now $\phi(x) = 0$ has no multiple root.

Consequently, as in Case I, the roots of $\phi(x) = 0$ between a and b is equal to the difference between the number of changes of sign in the sequence of ϕ's when $x = a$ and that when $x = b$. It is identical with the difference between the number of changes of sign in the sequence of f's when $x = a$ and that when $x = b$. Moreover, the roots of the equation $\phi(x) = 0$ are the same as those of the equation $f(x) = 0$, but the multiple roots of $f(x) = 0$ occur in $\phi(x) = 0$ once only.

Hence the theorem is completely proved.

Note. Calculation of Sturm's functions, particularly in the case of high degree polynomials, is very laborious. Some labour may be saved by the following considerations :

(*i*) In case of no multiple root, the last function $f_m(x)$ is independent of x and only its sign is required.

(*ii*) If the equation obtained by equating any one of Sturm's functions to zero has all the roots imaginary, then we need not calculate any function beyond that one.

(*iii*) If any one of the Sturm's functions be a perfect square, then we need not calculate any function beyond that one.

(*iv*) If one of Sturm's functions, say $f_r(x)$, vanishes when $x = a$, then in counting the number of changes of sign in the sequence

$$f(a), f_1(a), f_2(a), \ldots\ldots, f_m(a),$$

we may regard the sign of $f_r(a)$ as either + or −.

5.16. Approximate solution of numerical equations by Newton's method.

Polynomial equations having numerical coefficients may be solved to get approximate roots by this method. The method consists in retaining only the first two terms of the Taylor's expansion of a function and is applicable to numerical equations involving transcendental functions also.

Let α be a real root of the equation $f(x)=0$ such that

$$\alpha = a+h,$$

h being very small and the function $f(x)$ and its derivatives are continuous at $x=a$.

Then $f(a+h)=0$.

By Taylor's expansion,

$$f(a)+hf'(a)+\frac{h^2}{2!}f''(a)+\cdots\cdots=0.$$

Now h being very small, we neglect h^2 and higher powers of h and get

$$f(a)+hf'(a)=0$$

or, $$h=-\frac{f(a)}{f'(a)}$$

as the approximation to h. Substituting this value of h in $\alpha = a+h$, we get the first approximate root as

$$\alpha = a-\frac{f(a)}{f'(a)}.$$

The process is repeated to give approximation of any degree of accuracy.

Thus starting with $x=\alpha$, we may obtain the second approximation $x=\beta$ to the root as $\beta=\alpha-\frac{f(\alpha)}{f'(\alpha)}$ and so on.

5.17. Horner's method.

This method is applied in solving any numerical equation to find both the commensurable and incommensurable roots; in the former case, roots are found completely and in the latter case, the roots are found to any desired decimal place. The essence of the method consists in alternate diminution of roots and multiplication of the roots by 10.

By trial, we find first two consecutive integers a and $(a+1)$ between which a root lies. The roots are diminished by a and that root is made to lie between 0 and 1 in the transformed equation. The roots of this transformed equation are multiplied by 10 and that root in the newly transformed equation then lies between 0 and 10. Let it be found to lie between b and $(b+1)$, by trial. The roots are then diminished by b and the process is

repeated as many times as desired. If $a, b, c, \ldots\ldots$ be the successive integers by which the roots are diminished, the required root wil be $a \cdot bc \ldots\ldots$

The same process is applied for negative roots after changing the signs of the roots.

Note. In the process of multiplying the roots again and again by 10, the coefficients of the transformed equations become very large and after two or three such multiplications it becomes difficult to determine the greatest integer involved in the root at that stage. The *principle of trial divisor* provides an easy method for finding the numbers by which the roots are to be diminished at the next stage. This principle states that the required number is obtained by dividing the last coefficient by the last but one which is called the *trial divisor.*

In the illustrative example 4, we shall illustrate the whole operation of the method in a single tabular form and use the method of trial divisor.

5.18. Illustrative Examples.

Ex. 1. *Obtain a finite superior limit of the positive roots of the equation*

$$x^5 + 3x^4 + 3x^3 - 28x^2 - 61x + 18 = 0. \qquad [C.\ H.\ 1974]$$

Also find an inferior limit of the positive roots of the equation.

By Article 5.11 (*a*), we get $\left(\sqrt[3]{61}+1\right)$, that is, 5 as a suprior limit and by Article 5.11 (*b*), we get $\left(\frac{61}{1+3+3}+1\right)$, that is, 10 as a superior limit. Here 5 is smaller superior limit of the positive roots of the given equation.

To find inferior limit of the positive roots of the given equation $f(x) = 0$, we first find superior limit of the positive roots of the equation

$$f\left(\frac{1}{x}\right) = 0, \text{ that is, } 18x^5 - 61x^4 - 28x^3 + 3x^2 + 3x + 1 = 0.$$

$\left(\frac{61}{18}+1\right)$, that is, 5 is a superior limit of the positive roots of the equation $f\left(\frac{1}{x}\right) = 0$. Hence $\frac{1}{5}$ is an inferior limit of the positive roots of the given equation.

Note 1. We can find a superior limit by merely grouping the terms of the given equation as $x^4(x-5) + 4x^2(2x^2-7) + x(3x^2-61) + 18 = 0$.

Left hand side is positive for $x \geq 5$. Thus 5 is a superior limit of the positive roots of the given equation.

Note 2. To find a superior limit of positive roots of the given equation $f(x)=0$ by Newton's method, we have here

$$f(x)=x^5+3x^4+3x^3-28x^2-61x+18,$$

$$f'(x)=5x^4+12x^3+9x^2-56x-61,$$

$$f''(x)=20x^3+36x^2+18x-56,$$

$$f'''(x)=60x^2+72x+18,$$

$$f^{iv}(x)=120x+72,$$

$$f^{v}(x)=120.$$

Here $x=1$ makes $f^{v}(x), f^{iv}(x), f'''(x)$ and $f''(x)$ positive but it makes $f'(x)$ negative. Now $x=2$ makes $f'(x)$ positive but $f(x)$ negative.

Proceeding upwards and increasing the value of x by unity, we see that $f(3)$ is positive. Hence 3 is a superior limit of positive roots.

Ex. 2. *Use Fourier's method to separate the roots of the equation*

$$f(x)=2x^5+7x^4-40x^3-23x^2+38x-4=0.$$

Here
$$f'(x)=2(5x^4+14x^3-60x^2-23x+19),$$

$$f''(x)=2(20x^3+42x^2-120x-23),$$

$$f'''(x)=8(15x^2+21x-30),$$

$$f^{iv}(x)=8(30x+21),$$

$$f^{v}(x)=240.$$

Let us apply Newton's method to find the limits of the roots of the equation. First we consider a superior limit of positive roots and we start from $x=0$.

x	$f^{v}(x)$	$f^{iv}(x)$	$f'''(x)$	$f''(x)$	$f'(x)$	$f(x)$
0	+	+	−			
1	+	+	+	−		
2	+	+	+	+	−	
3	+	+	+	+	+	−
4	+	+	+	+	+	+

So 4 is a superior limit of positive roots and the greatest root of the equation $f(x)=0$ lies between 3 and 4.

Similarly, by considering the equation $f(-y)=0$, a superior limit for its positive roots is determined. The transformed equation is

$$\phi(y)=2y^5-7y^4-40y^3+23y^2+38y+4=0.$$

Now $\phi'(y)=2(5y^4-14y^3-60y^2+23y+19)$,

$\phi''(y)=2(20y^3-42y^2-120y+23)$,

$\phi'''(y)=8(15y^2-21y-30)$, $\phi^{iv}(y)=24(10y-7)$, $\phi^{v}(y)=240$.

The expression of $\phi^{iv}(y)$ suggests that we can start from $y=1$.

y	$\phi^{v}(y)$	$\phi^{iv}(y)$	$\phi'''(y)$	$\phi''(y)$	$\phi'(y)$	$\phi(y)$
1	+	+	−			
2	+	+	−			
3	+	+	+	−		
4	+	+	+	+	−	
5	+	+	+	+	+	−
6	+	+	+	+	+	−
7	+	+	+	+	+	+

So 7 is a superior limit of positive roots of $\phi(-y)=0$.

Therefore (-7) is an inferior limit to the negative roots of $f(x)=0$ and the least root lies between (-6) and (-7).

We now try to find all the roots of the equation $f(x)=0$ lying in the interval $(-7,4)$.

For various values of x, the signs of Fourier's functions are as follows:

x	$f(x)$	$f'(x)$	$f''(x)$	$f'''(x)$	$f^{iv}(x)$	$f^{v}(x)$	Number of changes of sign
-7	$-$	$+$	$-$	$+$	$-$	$+$	5
-6	$+$	$+$	$-$	$+$	$-$	$+$	4
-5	$+$	$+$	$-$	$+$	$-$	$+$	4
-4	$+$	$-$	$-$	$+$	$-$	$+$	4
-3	$+$	$-$	$+$	$+$	$-$	$+$	4
-2	$+$	$-$	$+$	$-$	$-$	$+$	4
-1	$-$	$-$	$+$	$-$	$-$	$+$	3
0	$-$	$+$	$-$	$-$	$+$	$+$	3
1	$-$	$-$	$-$	$+$	$+$	$+$	1
2	$-$	$-$	$+$	$+$	$+$	$+$	1
3	$-$	$+$	$+$	$+$	$+$	$+$	1
4	$+$	$+$	$+$	$+$	$+$	$+$	0

Thus we see that there is one root in each of the intervals $(-7,-6),(-2,-1),(3,4)$ and either two roots or none in the interval $(0,1)$.

Sub-dividing the last interval, we see that $f(0{\cdot}5)$ is positive.

Hence there is a root in each of the intervals $(0,0{\cdot}5)$ and $(0{\cdot}5,1)$.

Ex. 3. *Use Sturm's theorem to show that the equation*

$$x^4-3x^3-2x^2+7x+3=0$$

has one root between (-2) *and* (-1), *one root between* (-1) *and* 0 *and two roots between* 2 *and* 3.

Here $f(x) = x^4 - 3x^3 - 2x^2 + 7x + 3$;

$f_1(x) = 4x^3 - 9x^2 - 4x + 7$.

Other Sturm's functions are

$f_2(x) = 43x^2 - 72x - 69$, $f_3(x) = 83x - 191$ and $f_4(x) = 48074$.

The number of changes of sign in the series of Sturm's functions for various values of x are as follows :

x	$f(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$	Number of changes of sign
$-\infty$	+	−	+	−	+	4
−2	+	−	+	−	+	4
−1	−	−	+	−	+	3
0	+	+	−	−	+	2
2	+	−	−	−	+	2
3	+	+	+	+	+	0
∞	+	+	+	+	+	0

Hence the given equation $f(x) = 0$ has one root between (–2) and (–1), one root between (–1) and 0 and two roots between 2 and 3.

Ex. 4. *Find a root of the equation* $x^3 - 2x - 5 = 0$ *correct to two places of decimal by Newton's method of approximation.*

Here $f(x) = x^3 - 2x - 5$ so that $f'(x) = 3x^2 - 2$. We have $f(2) = -1$ and $f(3) = 16$. Hence a real root of the equation lies in (2,3).

Let us start with the value $x = 2$. The first approximate value of the root is

$$\alpha = 2 - \frac{f(2)}{f'(2)} = 2 - \frac{-1}{10} = 2{\cdot}1.$$

For the second approximation, we get

$$\beta = 2{\cdot}1 - \frac{f(2{\cdot}1)}{f'(2{\cdot}1)} = 2{\cdot}1 - \frac{0{\cdot}061}{11{\cdot}23}$$

$$= 2{\cdot}1 - 0{\cdot}0054 = 2{\cdot}0946.$$

For the third approximation, we get

$$\gamma = 2\cdot0946 - \frac{f(2\cdot0946)}{f'(2\cdot0946)} = 2\cdot09455\,.$$

Thus the root correct to two decimal places is 2·09.

Ex. 5. *Find, by Horner's method, the positive root of the equation* $x^3 + 3x - 7 = 0$, *to three decimal places.*

By trial, it is seen that the positive root lies between 1 and 2.

Then we proceed as follows :

1	0	3	−7	(1·406
	1	1	4	
1	1	4	−3000	
	1	2	2944	
1	2	600	−56000000	
	1	136		
1	30	736		
	4	152		
1	34	888000		
	4			
1	38			
	4			
1	4200			

Diminishing the roots by 1, the transformed equation becomes

$$x^3 + 3x^2 + 6x - 3 = 0\,,$$

whose roots when multiplied by 10, the transformed equation becomes

$$x^3 + 30x^2 + 600x - 3000 = 0\,.$$

These coefficients are below the first thick jointed line. By trial, its positive root is seen to lie between 4 and 5 and hence the roots are diminished by 4 and then multiplied by 10 again. The transformed equation as obtained from below the second thick jointed line is

$$x^3 + 420x^2 + 88800x - 56000 = 0\,.$$

The positive root of this equation lies between 0 and 1. The equation remains the same when the roots are diminished by zero. Then the roots are again multiplied by 10.

The next integer is obtained by trial divisor method and is

$$\frac{56000000}{8880000} = 6 \text{ (only the integral portion).}$$

Thus the root is 1·406 (approximately).

Examples V (C)

1. (*a*) Find a superior and an inferior limit of the positive roots of the equation $x^8 + 20x^7 + 4x^6 - 11x^5 - 120x^4 + 13x + 25 = 0$.

(*b*) Show that (-5) is a superior limit of the negative roots of the equation $x^4 - 2x^3 - 13x^2 + 38x - 24 = 0$.

[Group the terms of the equation accordingly.]

(*c*) Show, by Newton's method, that 10 is a superior limit of the positive roots of the equation $x^3 - 2x^2 - 51x - 110 = 0$.

(*d*) Find the limits of the roots of the equations

(*i*) $x^3 - 9x^2 + 13x - 23 = 0$.

(*ii*) $x^5 + x^4 + x^2 - 25x - 100 = 0$.

2. Apply Fourier's method of separate the roots of the equations

(*i*) $x^4 - x^3 - 4x^2 + 4x + 1 = 0$.

(*ii*) $x^5 + x^4 + x^2 - 25x - 36 = 0$.

3. Find Sturm's functions for the equation

$$x^3 + 11x^2 - 102x + 181 = 0.$$

4. (*a*) Use Sturm's theorem to prove that the equation $x^3 - 7x + 7 = 0$ has two roots between 1 and 2 and one root between (-4) and (-3).

[*K. H. 2005; V.H. 2006; C. H. 2008*]

(*b*) Use Sturm's theorem to show that the equation $x^3 - 2x - 5 = 0$ has one positive root and two imaginary roots. [*C.H. 2007*]

5. Find by Sturm's method, the number and positions of the real roots of the equations

(*i*) $x^3-3x+1=0$.

(*ii*) $x^4-2x^3-7x^2+10x+10=0$.

(*iii*) $x^5-10x^3+6x+1=0$.

(*iv*) $x^5-5x+1=0$.

(*v*) $x^6-7x^3+15x^2+3x-4=0$.

6. Find to two decimal places, by Newton's method of approximation, the root of the equation $x^3+x^2+x-100=0$ which is nearly equal to 4.

7. Find the positive root of the equation

$$4x^3+35x^2+57x-351=0.$$

8. Find, by Horner's method, the real positive root of the equation $8x^3-10x^2-3x-7=0$ which lies between 1 and 2.

9. Find the negative root of the equation

$x^4-12x^2+12x-3=0$ correct to four decimal places.

10. Find the positive root of the equation

$$2x^3-85x^2-85x-87=0.$$

11. Find the positive root of the equation $x^3-2x-5=0$ correct to three decimal places by Horner's method.

12. Find the real root of the equation $x^3+29x-97=0$ correct to four decimal places.

13. Find the negative root of the equation

$x^3-12x+8=0$ correct to three decimal places.

14. Find, by Horner's method, the root lying between 2 and 3 of the equation $x^4-12x^2+12x-3=0$, to six decimal places. [*B. H. 1962*]

15. Find the positive root of the equation $2x^3-3x-6=0$ correct to four decimal places.

Answers

1. *(a)* $6, \frac{1}{4}$. *(d) (i)* 9, 1. *(ii)* (3, 1), (−2, −3).

2. (*i*) One real root in each of the intervals $(-2,-1),(-1,0),(1,1\cdot5),(1\cdot5,2)$.

(*ii*) One real root in each of the intervals $(-3,-2),(-2,-1),(2,3)$ and two imaginary roots.

3. $\left(x^3+11x^2-102x+181\right),\left(3x^2+22x-102\right),\ (854x-2751),441.$

5. (*i*) All roots real; one each in the intervals (–2, –1), (0,1), (1, 2).

(*ii*) All roots real ; one each in the intervals (– 3, – 2), (– 1, 0) and two in (2, 3).

(*iii*) All roots real ; one each in the intervals (– 4, – 3), (0, 1), (3, 4) and two in (–1, 0).

(*iv*) One real root in each of the intervals (–2, –1), (0, 1), (1, 2) and two imaginary roots.

(*v*) Four real roots and all real roots in the interval (– 1, 1).

6. 4·26. **7.** 2·25. **8.** 1·75. **9.** – 3·9074.

10. 43·5. **11.** 2·095. **12.** 2·6807. **13.** – 3·759.

14. 2·858105. **15.** 1·7838.

3 GROUP THEORY

3.1. Introduction.

Theory of groups is one of the most important fundamental concepts of Modern Algebra. This theory has wide practical application in the study of crystal structure, configuration molecules and structure of human genes. It has been applied by Albert Einstein in his study of special theory of relativity. This mathematical structure is associated with a mathematical system in which the closure, identity, inverse and associative properties for the elements of a set concerning an operation has been combined. Group is an algebraic structure with only one binary operation.

3.2. Groupoid, semi-group and monoid.

Consider the algebraic structure (S, o) in which S is a non-empty set on which the binary composition o is defined. Thus S is closed with the operation o. Hence, if

$$a, b \in S, \text{ then } a o b \in S.$$

Such a system consisting of a non-empty set S and a binary composition o defined in S is called a *groupoid*, and is denoted by (S, o).

If N be the set of natural numbers, then $(N, +)$ is a groupoid, because the set N is closed under addition. But the set of odd integers is not a groupoid under addition composition. The set $S = \{-2, -1, 0, 1, 2\}$ is not a groupoid with respect to addition, since $2 + 2 = 4 \notin S$, that is, the set S is not closed with addition composition.

If the binary composition o be commutative in S, then the groupoid is said to be a *commutative groupoid* .

If $a \, o \, x = x$ for all $x \in S$, then $a \in S$ is called the left identity element of the groupoid. Similarly, $a \in S$ is a right identity element of the groupoid, if $x \, o \, a = x$ for all $x \in S$.

The groupoid $(Z, -)$ has no left identity element but zero is a right identity element of it. In $(Z, +)$, 0 is a left as well as right identity. In the groupoid $(Z, \cdot)$, 1 is the left as well as right identity. This is called the identity element of the groupoid.

If a groupoid possesses a right as well as a left identity, then they are equal.

If a groupoid (S, o) contains an identity element, then that element is unique.

A system consisting of a non-empty set S and an associative binary composition o in S is called a *semi-group*. Thus a groupoid (S, o) will be a semi-group, if o be associative.

Consider, for example, $a, b, c \in Z$, the set of all integers. Then we have $(a+b)+c = a+(b+c)$ and also $(a \,.\, b) \,.\, c = a \,.\, (b \,.\, c)$. Thus Z being closed with the operations of addition and multiplication, the systems $(Z, +)$, and $(Z, \cdot)$ are semi-groups as those two compositions are also associative in Z.

If, in a semi-group, the operation be commutative, then it is called a *commutative semi-group*. Z, Q, R, C are all commutative semi-groups with respect to addition and multiplication.

The system $(Z, -)$ is not a semi-group, since subtraction does not satisfy the associative law.

A system consisting of a non-empty set S and an associative binary composition with identity is called a *monoid*. Thus monoid is an associative groupoid with an identity element. If Z be the set of all integers, then $(Z,+)$ is a monoid with identity element 0 and $(Z, \cdot)$ is a monoid with 1 as the identity element. If E be the set of all even integers, the $(E, \cdot)$ is a semi-group but not a monoid.

3.3. Group.

A non-empty set S of elements $a, b, c, \ldots\ldots$ forms a *group* with repect to the binary operation $*$, if the following properties (axioms) hold :

(i) For every pair a and $b \in S$, $a * b$ is in S (closure law).

(ii) For any three elements $a, b, c \in S$,

$$a * (b * c) = (a * b) * c \text{ holds} \quad \text{(associative law)}.$$

(iii) There exists in S an element i, called a left identity, such that

$$i * a = a, \text{ for every } a \in S.$$

(iv) For each a in S, the equation $x * a = i$ has a solution x in S.

This solution x is called a *left inverse* of a.

If, in addition to these postulates for a group,

$$a * b = b * a \qquad \text{(commutative law)},$$

for all a and b in the group, then the group is called a *commutative* or an *abelian* group; otherwise, it is called a *non-abelian* group.

For example, consider the set of integers (positive, negative and zero)

$Z = \{\ldots\ldots, -2, -1, 0, 1, 2, \ldots\ldots\}$,

on which the binary operation addition is applied.

For any $a, b, c \in Z$, we have

(i) $a + b \in Z$ (closure)

(ii) $(a + b) + c = a + (b + c)$ (associativity),

(iii) $0 + a = a$ (0 is the left identity element),

(iv) $(-a) + a = 0$ (left inverse of a is $-a \in Z$).

Hence the set of integers forms a group with respect to addition, since it satisfies all the group axioms.

Moreover $a + b = b + a$, which shows that it is an abelian group.

Thus the set Z of all integers (positive, negative including zero) with additive binary operation is an abelian group.

Consider, again, the set Q^+ of non-zero rational numbers, on which the binary operation multiplication is applied.

For any $a, b, c \in Q^+$, we have

(i) $a \times b \in Q^+$ (closure),

(ii) $(a \times b) \times c = a \times (b \times c)$ (associativity),

(iii) $1 \times a = a$ (1 is the left identity element),

(iv) $\frac{1}{a} \times a = 1$ $\left(\frac{1}{a}\right.$ is the left inverse of $\left.a\right)$.

Moreover $a \times b = b \times a$.

Hence the set Q^+ of non-zero rational numbers is an abelian group with respect to multiplication.

If Q be the set of rational numbers, then $(Q, +)$ is an abelian group but $(Q, \cdot)$ is not, since 0 has no left inverse in Q.

A group with addition binary operation is known as *additive* group and that with multiplication binary operation is known as *multiplicative* group.

A group for the binary operation $*$ is often written as $(G, *)$ or $<G, *>$, where G refers to the set forming the group. If the underlying set in a group consists of a finite number of elements, then it is called a *finite group*; the number of elements in the underlying set determines its *order*.

Thus the order of a finite group is the number of its elements. An *infinite group* consists of infinite number of elements in its underlying set. It is said to be of order zero or of infinite order.

Generally, the order of the group G is denoted by $o(G)$.

$(Z,+)$ is an infinite group, while $G = \{1, -1, i, -i\}$ is a finite group under multiplication whose $o(G)$ is 4.

Sometimes only the set symbol G is used to denote a group in context of a given operation.

3.4. Elementary theorems on groups.

Theorem 1. *Let a, b, c be arbitrary elements of a group $(G,*)$. If $a*b = a*c$, then $b = c$.*

In the group $(G,*)$, let a left inverse of a be $a' \in G$.

Then $a'*a = i$, where $i \in G$ is a left identity element.

Since $a*b = a*c$, operating on the left with a', we get

$$a'*(a*b) = a'*(a*c)$$

or, $$(a'*a)*b = (a'*a)*c \qquad \text{(associativity)}$$

or, $$i*b = i*c$$

or, $$b = c.$$

This law is known as *left cancellation law.*

Theorem 2. *In a group $(G,*)$, a left identity element is also a right identity element, that is, $i*a = a*i = a$, for every a in G.*

Let a' be a left inverse of a.

Then $a'*(a*i) = (a'*a)*i = i*i = i = a'*a$.

Thus, by the previous theorem, $a*i = a$, for every $a \in G$.

Hence a left identity i is also a right identity.

Henceforth we shall drop the qualifying words left and right and use the term identity element.

Theorem 3. *In a group $(G,*)$, a left inverse a' of an element a is also the right inverse of a, that is,*

$$a'*a = a*a' = i \qquad \text{(identity element)}$$

We have $a'*(a*a') = (a'*a)*a'$ (associativity)

$= i*a'$ (left inverse exists)

$= a'*i,$ by Theorem 2

Thus $a'*(a*a') = a'*i.$

Therefore $a*a' = i,$ by Theorem 1.

Thus the left inverse of an element in a group is also its right inverse. Henceforth we shall drop the qualifying words left and right and use the term inverse of an element.

Cor. we are now in a position to define a group in the following way : A non-empty set S of elements $a, b, c,.....$ forms a group with respect to the binary operation $*$, if the following properties (axioms) hold :

(i) For every pair a and $b \in S$, $a*b$ is in S (closure law).

(ii) For any three elements $a, b, c \in S$,

$a*(b*c) = (a*b)*c$ holds (associative law).

(iii) There exists in S an element i, called the *identity* element , such that $i*a = a = a*i$, for every $a \in S$.

(iv) For each a in S, the equation $x*a = i = a*x$ has a solution in S. This solution x is called the *inverse* of a.

Theorem 4. *The identity element of a group $(G,*)$ is unique.*

If the identity element be not unique, let i and e be two identity elements of $(G,*)$.

Hence $i*e = e*i = e,$

since i is an identity element and $e \in G$.

Again $e*i = i*e = i,$

since e is an identity element and $i \in G$.

Therefore $e = i,$

that is, the identity element of a group is unique.

Theorem 5. *Each element in a group $(G,*)$ has a unique inverse.*

Let the element $a \in G$. If the inverse of the element a be not unique, let a' and a'' be the two inverses of a for $*$ in G. Let i be the identity element for $*$ in G.

Since a' is an inverse of a, then $a'*a = a*a' = i.$ ... (1)

Since a'' is an inverse of a, then $a''*a = a*a'' = i.$ ... (2)

Now $a'' = i * a'' = (a' * a) * a'' = a' * (a * a'')$ (associativity)

$= a' * i = a'$.

Thus the inverse of an element in a group is unique.

Note. From (1) and (2), we have $a * a' = a * a''$.

Then, by left cancellation law, we have $a' = a''$.

Henceforth we shall denote the unique inverse of an element a by the symbol a^{-1}.

Theorem 6. *Let a, b, c be three arbitrary elements of a group $(G, *)$.*

If $a * c = b * c$, then $a = b$.

Given $a * c = b * c$;

operating on the right with c^{-1}, the inverse of c, we get

$$(a * c) * c^{-1} = (b * c) * c^{-1}$$

or, $a * (c * c^{-1}) = b * (c * c^{-1})$ (associativity)

or, $a * i = b * i$, (i is the identity)

i being the identity element, we have $a = b$.

This law is known as *right cancellation law.*

Theorem 7. *In a group $(G, *)$,*

(i) the inverse of the inverse of an element is equal to the element ;

(ii) the inverse of the product of two elements is the product of the inverses in the reverse order.

Thus, if $a, b \in G$, then we are to show that

(i) $(a^{-1})^{-1} = a$ and *(ii)* $(a * b)^{-1} = b^{-1} * a^{-1}$.

(i) Let i be the identity element for $*$ in G.

Then we have $a * a^{-1} = i$, where $a^{-1} \in G$.

Also we have $(a^{-1})^{-1} * a^{-1} = i$.

Therefore $(a^{-1})^{-1} * a^{-1} = a * a^{-1}$.

Thus, by right cancellation law, we have $(a^{-1})^{-1} = a$.

(ii) Again, since a and $b \in G$ and G is a group for $*$, then

$a * b \in G$ (closure).

Therefore $(a * b)^{-1} * (a * b) = i$. ... (1)

Let a^{-1} and b^{-1} be the inverses of a and b respectively ; then

$$a^{-1}, b^{-1} \in G.$$

Therefore $\left(b^{-1} * a^{-1}\right) * (a * b) = b^{-1} * \left(a^{-1} * a\right) * b$ (associativity)

$$= b^{-1} * i * b = b^{-1} * b = i. \quad \ldots \quad (2)$$

From (1) and (2) and right cancellation law, we have

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

Note. In general,

$$(a * b * c * \ldots\ldots * p * q)^{-1} = q^{-1} * p^{-1} * \ldots\ldots * c^{-1} * b^{-1} * a^{-1}.$$

Theorem 8. *In a group* $(G, *)$, *the equations*

$$a * x = b \text{ and } y * a = b$$

have unique solutions for the unknowns x *and* y ; *the solutions are* $x = a^{-1} * b$ *and* $y = b * a^{-1}$, *where* $a, b \in G$.

If possible, let the equation $a * x = b$ have two solutions x and x' *in* G.

Then $a * x = b$ and $a * x' = b$.

Therefore $a * x = a * x'$, where $a, x, x' \in G$.

By left cancellation law, we have $x = x'$.

Again, assuming $x = a^{-1} * b$, we have

$$a * x = a * \left(a^{-1} * b\right)$$

$$= \left(a * a^{-1}\right) * b \quad \text{(associativity)}$$

$$= i * b \quad (i \text{ being the identity element})$$

$$= b.$$

This shows that $x = a^{-1} * b$ satisfies the equation $a * x = b$.

The second part can similarly be proved.

Note. The solvability of the equation $a * x = b, a, b \in$ a finite set S on which the operation $*$ is defined, implies that the row a in the composition table must contain b once if the solution be unique and more than once if it be not unique. Similar consideration should be made for the solvability and uniqueness of the solution of the equation $y * a = b$ from the entries along the column of a.

The equations will have no solution, if the corresponding row or column does not contain b.

Theorem 9. *Let* $\{G,*\}$ *be a semi-group and for* $a,b \in G$ *each of the equations*

$$a*x=b \text{ and } y*a=b$$

has a solution in G. Then $\{G,*\}$ *is a group.*

Since $\{G,*\}$ is a semi-grup, G is closed under the composition $*$ and $*$ is associative for all elements of G.

Let e and $e' \in G$ satisfy the equations

$$a*x=a \text{ and } y*a=a \text{ respectively.}$$

Therefore $a*e=a$ and $e'*a=a$.

Let c be an arbitrary element in G and $m,n \in G$ be respectively the solutions of

$$a*x=c \text{ and } y*a=c.$$

Therefore $a*m=c$ and $n*a=c$.

Now
$$\begin{aligned} c*e &= (n*a)*e \\ &= n*(a*e), \text{ since } * \text{ is associative} \\ &= n*a \\ &= c. \end{aligned}$$

But c being arbitrary, $a*e=a$, for all $a \in G$. ... (1)

Again
$$\begin{aligned} e'*c &= e'*(a*m) \\ &= (e'*a)*m, \text{ since } * \text{ is associative} \\ &= a*m \\ &= c. \end{aligned}$$

But c being arbitrary, $e'*a=a$, for all $a \in G$. ... (2)

From (1), we have $e'*e=e'$ and from (2), we have

$$e'*e=e.$$

Thus $e=e'$.

Hence, for $e \in G$, we have $e*a=a*e=a$, for all $a \in G$. ... (3)

Let again a' and a'' be elements in G which are the solutions of

$$a*x=e \text{ and } y*a=e.$$

Therefore $a*a'=e$ and $a''*a=e$.

But $*$ being associative, we have

$$(a'' * a) * a' = a'' * (a * a').$$

Hence $e * a' = a'' * e,$

that is, $a' = a''.$

Thus, for each $a \in G$, there is an element $a' \in G$, such that

$$a' * a = a * a' = e. \quad \ldots (4)$$

Hence, in view of (3) and (4), the semi-group $\{G, *\}$ is a group.

Theorem 10. *Let $\{G, *\}$ be a semi-group containing a finite number of elements in which right as well as left cancellation laws hold. Then $\{G, *\}$ is a group.*

For all $a, b, c \in G$, we have

$$a * b = a * c \Rightarrow b = c$$

and $b * a = c * a \Rightarrow b = c.$

Let the set G consist of the n elements

$$a_1, a_2, a_3, \ldots\ldots, a_n.$$

Consider now the elements

$$a_1 * a_1, a_1 * a_2, \ldots\ldots, a_1 * a_n.$$

These elements belong to G and are distinct. If they are not distinct, let

$$a_1 * a_i = a_1 * a_j.$$

Then, by cancellation law, $a_i = a_j$; which contradicts the fact that the n elements $a_1, a_2, \ldots\ldots, a_n$ of the set G are distinct.

The n composite elements

$$a_1 * a_1, a_1 * a_2, \ldots\ldots, a_1 * a_n$$

being all distinct, they are the n given elements of G in some order.

This shows that the equation

$$a * x = b, \quad a, b \in G$$

has a solution in G.

Similarly, by forming the products

$$a_1 * a_1, a_2 * a_1, \ldots\ldots, a_n * a_1,$$

it can be shown that the equation

$$y * a = b, \quad a, b \in G$$

has a solution in G.

Thus $\{G, *\}$ is a semi-group, in which each of the equations $a * x = b$ and $y * a = b$ has a solution in G, for all $a, b \in G$.

Hence $\{G, *\}$ is a group.

Note. This theorem does not hold if G contains an infinite number of elements.

3.5. Quasi-group and Klein's 4 - group.

A groupoid (S, o) is said to be a *quasi-group*, if, for any two elements $a, b \in S$, each of the equations

$$a o x = b \text{ and } y o a = b$$

has a unique solution in S.

For example, the groupoid $(Z, +)$ is a quasi-group. This is because for any two elements $a, b \in Z$, we have the unique solution $x = b - a$ in Z for the equation $a + x = b$ and $y = b - a$ in Z for the equation $y + a = b$.

But $(Z, \cdot)$, although a groupsoid, is not a quasi-group; for, the equations $3 \cdot x = 2$ and $y \cdot 3 = 2$ will have no solutions in Z, but $3, 2 \in Z$.

$(Z, -)$ is a quasi-group but not a semi-group.

Consider the finite set $S = \{e, a, b, c\}$, on which the binary operation $*$ is defined as in the composition table given below :

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

It is clear that $\{S, *\}$ is an abelian group of order 4, each element of the group being its own inverse and e being the identity of the binary operation.

This is known as *Klein's 4 - group.*

3.6. Quaternion groups.

Consider the finite set $G = \{\pm e, \pm i, \pm j, \pm k\}$, on which the binary operation $*$ is defined as in the composition table given below :

$*$	e	$-e$	i	j	k	$-i$	$-j$	$-k$
e	e	$-e$	i	j	k	$-i$	$-j$	$-k$
$-e$	$-e$	e	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	$-e$	k	$-j$	e	$-k$	j
j	j	$-j$	$-k$	$-e$	i	k	e	$-i$
k	k	$-k$	j	$-i$	$-e$	$-j$	i	e
$-i$	$-i$	i	e	$-k$	j	$-e$	k	$-j$
$-j$	$-j$	j	k	e	$-i$	$-k$	$-e$	i
$-k$	$-k$	k	$-j$	i	e	j	$-i$	$-e$

From the composition table, it is clear that closure property and associative property hold good for the binary operation $*$. e is the identity of the binary operation and $i^{-1} = -i$, $j^{-1} = -j$, $k^{-1} = -k$ and $e^{-1} = -e$.

Thus $\{G, *\}$ is a group of order 8. This is known as *quaternion group*.

This is not an abelian group.

For example, the set of eight complex matrices

$$\left\{\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \pm\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, \pm\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}, \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\right\}, \text{ where } i^2 = -1,$$

forms a quaternion group under matrix multiplication and this group is called the *group of unit quaternions* and is denoted by Q_8.

3.7. Illustrative Examples.

Ex. 1. (*a*) *If a groupoid* (S, o) *contains an identity element, then show that it is unique.*

(*b*) *Show that* $\{M_2, +\}$ *and* $\{M_2, \cdot\}$ *are semi-groups, where* M_2 *denotes the set of all real* 2×2 *square matrices and* $+$ *denotes matrix addition and* $\cdot$ *denotes matrix multiplication.*

(*a*) If possible, let there be two identity elements e and e' in (S, o).

Hence $e o e' = e' o e = e'$, since e is an identity element and $e' \in S$.

Again $e' o e = e o e' = e$, since e' is an identity element and $e \in S$.

Therefore $e = e'$,

that is, the identity element of a groupoid is unique.

(*b*) Let $M_2 = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a, b, c, d \in R$.

We know that the matrix sum of two real matrices is a real matrix of the same order.

Also the matrix addition is associative.

Hence $\{M_2, +\}$ is a semi-group.

Similarly, it can be shown that $\{M_2, \cdot\}$ is a semi-group.

Ex. 2. *Show that the set of cube roots of unity is a finite abelian group with respect to multiplication.* [B.H. 2001]

The set of cube roots of unity is $S = \{1, \omega, \omega^2\}$.

(*i*) Closure axiom is satisfied, since

$$1 \cdot \omega = \omega, \quad \omega \cdot \omega^2 = 1, \quad \omega^2 \cdot 1 = \omega^2.$$

(*ii*) Associative axiom is satisfied, since

$$(1 \cdot \omega) \cdot \omega^2 = 1 \cdot (\omega \cdot \omega^2), \text{ etc.}$$

(*iii*) Identity axiom is satisfied, since

$$1 \cdot \omega = \omega, \; 1 \cdot \omega^2 = \omega^2, \; 1 \cdot 1 = 1.$$ 1 is the identity element.

(*iv*) Inverse axiom is satisfied, since

$$1 \cdot 1 = 1 = \omega \cdot \omega^2 = \omega^2 \cdot \omega$$

(inverse of each element exists in the set).

(*v*) Commutative property is satisfied, since

$$1 \cdot \omega = \omega \cdot 1, \; \omega \cdot \omega^2 = \omega^2 \cdot \omega, \text{ etc.}$$

Moreover the number of elements of S is finite.

Hence the set S forms a finite abelian group with respect to multiplication.

Ex. 3. *Check the following multiplication table for the set of fourth roots of unity, namely* $\{1,-1,i,-i\}$ *for its group properties :*

×	1	−1	i	$-i$
1	1	−1	i	$-i$
−1	−1	1	$-i$	i
i	i	$-i$	−1	1
$-i$	$-i$	i	1	−1

[*B.H. 1983 ; C.H.1994*]

We see from the composition table that

(*i*) the closure property holds, since

$1\times1=1,\ -1\times i=-i,\ i\times(-i)=1$, etc ;

(*ii*) the operation is associative, since

$(1\times i)\times(-i)=1\times[i\times(-i)]=1$, etc;

(*iii*) the set has 1 as the identity element with respect to the given operation, since $1\times(-1)=-1,\ 1\times i=i,\ 1\times(-i)=-i$, etc ;

(*iv*) each element has an inverse, since

$1\times1=1,\ (-1)\times(-1)=1,\ -i\times i=1,\ i\times(-i)=1$, etc.

Hence the set forms a multiplicative group. The set is commutative with respect to multiplication ; for, $1\times(-1)=(-1)\times1,\ (-1)\times i=i\times(-1)$, etc.

Hence it forms an abelian group.

Note. It is seen that a group is commutative, if the composition table with the corresponding operation has a symmetry across its leading diagonal.

Ex. 4. *If* a *be an element of a multiplicative group with identity element* e *and if* $a^2=a$, *then show that* $a=e$.

Since a is an element of the group, it has its inverse, say a^{-1}, in the group.

Operating both sides of the given equation by a^{-1} on the right, we have

$$(a^2)a^{-1}=aa^{-1}$$

that is, $(aa)a^{-1}=aa^{-1}$

or, $a(aa^{-1})=e$, the identity element

or, $ae=e$, which gives $a=e$, since $a^2=a$.

Ex. 5. *Show that the following four matrices form a group under matrix multiplication :*

$$A=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix},\quad B=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix},\quad C=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},\quad D=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}.$$

We see that A is a unit matrix.

Hence $AA=A,\ AB=BA=B, AC=CA=C, AD=DA=D$.

Also $BC=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix}=D$ and $BD=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=C$.

Similarly, $CB=D$ and $DB=C$.

Again $DC=CD=B$.

Also $BB=CC=DD=A$.

Hence we find the composition table as

$\times$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

The set of four matrices is thus closed with respect to matrix multiplication. The elements are associative for the operation. A is the identity element and every element is its own inverse as seen from the table. Thus the set of the four matrices forms a multiplicative group which is commutative as well.

Ex. 6. *Show that if every element of a group (G, o) be its own inverse, then it is an abelian group.* [B.H. 1987]

Is the converse true ?

Let $a, b \in G$; then $a \circ b \in G$ (closure).

Hence, by the given condition, we have

$$\begin{aligned} a \circ b &= (a \circ b)^{-1} \\ &= b^{-1} \circ a^{-1} \\ &= b \circ a, \text{ since } a^{-1} = a \text{ and } b^{-1} = b. \end{aligned}$$

Thus $a \circ b = b \circ a$, for every $a, b \in G$.

Therefore it is an abelian group.

The converse is not true. For example, $(R, +)$, where R is the set of all real numbers, is an abelian group, but no element except 0 is its own inverse.

Ex. 7. *Prove that a group with three elements is necessarily abelian.*

Let $G = \{a, b, i\}$ form a group under certain operation o, i being the identity. Indeed $i^{-1} = i$.

If further $a^{-1} = a$ and $b^{-1} = b$, then, by the previous example, the group formed is abelian.

Now consider that $a^{-1} \neq a$ and $b^{-1} \neq b$. But since G forms a group, therefore the other possibilities are

$$a^{-1} = i \text{ or } a^{-1} = b \text{ and } b^{-1} = i \text{ or } b^{-1} = a.$$

Now $a^{-1} = i \Rightarrow \left(a^{-1}\right)^{-1} = i$ or $a = i$.

But a and i are distinct elements of G; therefore we cannot have $a^{-1} = i$.

Hence we must have $a^{-1} = b$.

Similarly, we must have $b^{-1} = a$.

Therefore $a \; o \; b = a \; o \; a^{-1} = i$

and $b \; o \; a = b \; o \; b^{-1} = i$.

Hence $a \; o \; b = b \; o \; a$.

Furthermore we have $a \; o \; i = a = i \; o \; a$ and $b \; o \; i = b = i \; o \; b$.

Thus every pair of elements commute. Hence G forms an abelian group.

Ex. 8. (*a*) *Show that the set Z of all integers does not form a group under the operation defined as*

$$x * y = x - y \text{ , for every } x, y \in Z. \qquad [B.H.\ 1987]$$

(*b*) *Show that the set Z of all integers forms a group under the binary operation* $*$ *defined by*

$$a * b = a + b + 1, \; a, b \in Z. \qquad [T.H.\ 2009]$$

(*a*) Let $Z = \{\ldots\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\ldots\}$.

Closure: $4 * 3 = 4 - 3 \in Z$, etc.

Associativity: $(4 * 5) * 6 = (4 - 5) * 6 = -1 * 6 = -1 - 6 = -7$.

Again $4 * (5 * 6) = 4 * (5 - 6) = 4 * (-1) = 4 - (-1) = 5$.

Therefore associativity does not hold. Hence the set Z does not form a group, although the set satisfies the closure property.

(*b*) For $a, b \in Z$, we have $a * b = a + b + 1 \in Z$,

which proves the closure property of the composition.

For the elements $a, b, c \in Z$,

$$(a * b) * c = (a + b + 1) * c = a + b + 1 + c + 1 = a + b + c + 2$$

and $$a * (b * c) = a * (b + c + 1) = a + b + c + 1 + 1 = a + b + c + 2.$$

Hence $$(a * b) * c = a * (b * c)$$

and the composition is associative.

Let e be an element of Z, such that $e * a = a$.

Therefore $e = -1$.

Now $-1 \in Z$; hence (–1) is the identity element.

If $a \in Z$, then $b \in Z$ will be the left inverse of a

if $b * a = -1$.

Hence $b + a + 1 = -1$, so that $b = -a - 2$.

Thus $(-a - 2)$ is the left inverse of a.

It is also commutative, since $a * b = a + b + 1 = b + a + 1 = b * a$.

Thus the set Z of all integers is an abelian group for the given composition.

Ex. 9. *Show that the set* $S = \{1, 2, 3, 4\}$ *forms a group for the operation multiplication modulo 5.*

× mod 5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

From the table, it is seen that

(*i*) *S* is closed with respect to the given operation, since the number obtained by the operation multiplication modulo 5 is an element of *S*; for instance, $2 \times 4 \pmod 5 = 3 \in S$, etc.

(*ii*) The operation is associative, since for all $a, b, c \in S$, each of $\{(a \times b) \times c\}$ and $\{a \times (b \times c)\}$ has the same positive remainder when divided by 5;

for instance,

$(2\times3)\times4 = 1\times4 = 4 \pmod 5$ and $2\times(3\times4) = 2\times2 = 4 \pmod 5$.

(*iii*) Obviously, the identity element is 1.

(*iv*) Every element has an inverse; for instance, $2\times3 = 1 = 3\times2 \pmod 5$.

Moreover, it can be verified that for all $a, b \in S$,

$a\times b = b\times a$; for instance, $4\times3 = 2 = 3\times4 \pmod 5$.

Therefore S forms an abelian group for multiplication modulo 5.

Ex. 10. *Show that the set of residue classes modulo 5 forms a group with respect to addition of residue classes, but it does not form a group with respect to multiplication of residue classes.*

Here we have $I_5 = \{[0],[1],[2],[3],[4]\}$.

We know that the sum and the product of the residue classes do not depend upon the particular notations used, but only upon the classes themselves. Thus, omitting the brackets, we construct the addition and the multiplication tables for I_5.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the first table, we see that I_5 is closed under addition of residue classes. The associative law holds for I_5 as it holds for the set of integers. The identity element is clearly 0 and the inverses of 0, 1, 2, 3, 4 are respectively 0, 4, 3, 2, 1.

Therefore I_5 forms a group under addition of residue classes.

From the second table, we see that closure, associative and identity axioms hold for the set I_5 under multiplication of residue classes, the identity element being 1. But the element 0 has no inverse, since $0\cdot a \not\equiv 1 \pmod 5$ for any a. Hence the set I_5 does not form a group with respect to multiplication of residue classes.

Examples III (A)

1. (*a*) Satisfy yourself that

(*i*) in the groupoid $(I,\bullet)$, 1 is both left and right identity element.

(*ii*) $(R, +)$ is a semi-goup, where R is the set of all real numbers.

(*iii*) the system $S = (Z, o)$, where $a\,o\,b = a+b+ab$, for all $a,b \in Z$ is a monoid.

(*iv*) the set of even integers forms a semi-group under the composition multiplication but does not form a monoid.

(*v*) the systems $(M_2, +)$ and $(M_2,\bullet)$ are monoids, where M_2 denotes the set of all real 2×2 matrices; $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ is the identity of the former and $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ is that of the latter.

(*vi*) the power set $P(S)$ is a monoid with respect to the compositions

$A\,o\,B = A\cap B$ and $A\,o\,B = A\cup B$. [K.H. 1977]

(*b*) If M be the set of all real matrices $\left\{\begin{bmatrix}a & a\\ b & b\end{bmatrix}; a+b\neq 0\right\}$, then show that $(M,\bullet)$ is a semi-group, where $\bullet$ denotes matrix multiplication. Show further that it has no left identity and $\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}$ is the right identity.

2. (*a*) Show that the set of all real numbers is a groupoid but not a semi-group under the operation o defined by

$$a\,o\,b = a+3b \qquad \forall\ a,b\in R.$$

But, if the binary operation o be defined by

$$a\,o\,b = b \qquad \forall\ a,b\in R,$$

then the set of real numbers forms a semi-group.

(*b*) Show that a quasi-group, in which the associative property holds, is a group. [K.H.1990]

(*c*) If (S, o) be a semi-group and $a \in S$, then prove that

$$a^{m+n} = a^m\ o\ a^n, \text{ for all } m,n\in N.$$

(*d*) Prove that the set $R \times R$ together with the operation o defined by $(a,b)o(c,d) = (a+c, b+d+2bd)$ is a commutative semi-group with identity. [*N.B.H. 2002*]

3. Prove that the set of even integers (including zero) forms an additive group.

Show further that the group is abelian. If the set be of odd integers, then prove that it does not form a group with respect to the composition addition.

4. (*a*) Show that the set of all rational numbers does not form a group with respect to multiplication. [*C.H. 1983*]

[It does not contain the inverse of 0.]

(*b*) If, in a group $G, x^2 = e$ (identity) for every $x \in G$, then prove that G is abelian. [*K.H. 1990*]

5. Show that the set of all non-zero integers does not form a group with the binary operations multiplication and subtraction.

6. Show that the set $S = \{-1, 0, 1\}$ does not form a group with respect to operations addition and multiplication, while the set $T = \{-1, 1\}$ is an abelian group under multiplication and does not form a group under addition.

7. Show that the set $S = \{-3, -2, -1, 0, 1, 2, 3\}$ is not a group with the operation addition.

8. Show that the set of positive integers does not form a group under the composition addition and the set of negative integers does not form a group with addition and multiplication.

9. Show that the set of non-zero real numbers forms a group with respect to multiplication. Show that this is also true for a set of non-zero complex numbers.

10. If $G = \{0\}$ be a singleton with 0 as its unity element, then show that it forms a group with additive property.

11. Show that the n-th roots of unity form an abelian group under ordinary multipication. [*B.H.1985*]

[By De Moivre's theorem, $1^{\frac{1}{n}} = e^{\frac{2\pi ri}{n}}$, where $r = 0, 1, 2, \ldots\ldots, (n-1)$.

Identity element is $e^{\frac{2\pi i 0}{n}} = 1$ and inverse of $e^{\frac{2\pi ir}{n}}$ is $e^{\frac{2\pi i(n-r)}{n}}$.]

12. Prove that the set of all $m \times n$ matrices having their elements as integers (rationals, reals) is an infinite abelian group with matrix addition as compostion.

13. (*a*) Prove that the set of all 2×2 non-singular matrices M_2 having their elements as real numbers is a non-abelian group with matrix multiplication as composition.

Show further that if some elements of M_2 be non-singular, then $\{M_2, \cdot\}$ is not a quasi-group, where $\cdot$ denotes matrix multiplication.

(*b*) Show that the set M of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where a, b, c, d are integers and $ad - bc = 1$, is a non-commutative group with respect to matrix multiplication. [C.H. 1992]

14. (*a*) Show that the set $\{a + \sqrt{2}b : a, b \in Q\}$, where Q is the set of rational numbers, forms a group under ordinary addition as composition.

(*b*) On the set of integers Z, the binary operation $*$ is defined as $a * b = a + b - 2$, for all $a, b \in Z$. Show that $< Z\ * >$ is a group.

15. Show that the set

(*i*) $\ldots\ldots, 2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, 2^4, \ldots\ldots$

forms a multiplicative group ;

and (*ii*) $\ldots\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots,$

where m is a fixed integer, forms an additive group.

16. Show that in the first two composition tables, the underlying sets do not form groups because in the first there is no inverse of a and in the second there is no identity element ; but the set of the third table forms a group with composition o.

$\times$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

$\cdot$	a	b	c	d
a	c	d	b	a
b	a	b	c	d
c	d	c	a	b
d	b	c	a	d

o	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

17. Prove that the six matrices

$$\begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}, \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \text{ for } \theta = 0, \tfrac{2}{3}\pi, \tfrac{4}{3}\pi$$

form a group with respect to usual matrix multiplication.

18. (*a*) Show that the set of matrices

$$A_\alpha = \begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix},$$

where α is a real number, forms a group under matrix multiplication.

(*b*) Prove that the set of all real orthogonal matrices of order n forms a group with respect to matrix multiplication. [*B.H. 1993*]

(*c*) Show that the set of all real matrices of the form $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$, where $a \neq 0$, forms a commutative group with respect to matrix multiplication.

(*d*) Show that the set

$$M = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$$

forms an abelian group under matrix multiplication. [*T.H. 2007*]

(*e*) If $G = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \text{ is any non-zero real number} \right\}$, then show that G forms a commutative group under matrix multiplication.

(*f*) Let G be the set of all 2×2 matrices $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, where a, b are real numbers and are not zero simultaneously. Show that G is a group with respect to multiplication.

(*g*) Show that the set of all complex numbers z with $|z| = 1$ is a group with respect to multiplication.

19. (*a*) Show that the set Q of all rational numbers, other than 1, forms a group under the binary operation $*$ defined by

$$a * b = a + b - ab, \quad a, b \in Q.$$

(*b*) In the set Q of rational numbers, the operation $*$ is defined by $a * b = a - b + a \cdot b$, where $+, \cdot, -$ denote the usual operations in Q. Show that $(Q, *)$ has no identity. [*C.H. 1984*]

(*c*) Prove that the set Z_0 of all odd integers forms a group with respect to the composition $*$ defined by

$$a * b = a + b - 3, \quad a, b \in Z_0.$$ [*B.H. 2002*]

(*d*) Show that the set G of all ordered pairs (a, b) with $a \neq 0$, of rational numbers a, b is a group with operation $*$ defined by

$$(a,b)*(c,d)=(ac,\ bc+d).$$ [C.H. 1990, 1996]

[Identity = (1, 0) and $\left(a^{-1}, -ba^{-1}\right)$ is the inverse of (a, b).]

20. Show that the set Q of all rational numbers, other than (-1), forms a group under the binary operation $*$ defined by

$$a*b=a+b+ab,\ a,b\in Q.$$

With the same definition of the operation $*$, when $a,b\in R$, show that $(R,*)$ is a monoid, but not a quasi-group.

21. $*$ is a binary operation in Q defined by $a*b=\frac{ab}{3}$, $a,b\in Q$ (the set of all positive rational numbers). Show that $(Q,*)$ is a commutative group. [V.H. 1987; B.H. 1995; N.B.H. 2006]

22. Show that the positive rationals do not form a group G with respect to the binary operation $*$ defined by $x*y=\frac{x}{y}$, $x,y\in G$.

23. (*a*) If, in a group (G, o), the elements a and b of G commute, then show that (*i*) $a^{-1}o\ b^{-1}=b^{-1}o\ a^{-1}$, (*ii*) $a^{-1}o\ b=b\ o\ a^{-1}$.

(*b*) Prove that the group (G, o) is abelian, if $a,b\in G$, $b^{-1}o\ a^{-1}o\ bo\ a=i$, where i is the identity of the group.

(*c*) If G be a group with binary operation $*$, then show that

$$\left(a*b^{-1}*c\right)^{-1}=c^{-1}*b*a^{-1},\ \text{for all } a,b,c\in G.$$

(*d*) Prove that a group with four elements is necessarily abelian under any binary operation. [V.H. 1997]

(*e*) If the set $\{1,x,y\}$ forms a multiplicative group, then show that $(xy)^{-1}=xy$ and $x^3=y^3=1$. [B.H. 1990]

24. Show that the set $G = \{0, 1, 2, 3\}$ forms a group with respect to addition modulo 4; but it does not form a group under multiplication modulo 4 as some of the elements have no inverses.

25. Show that the set $S = \{0, 1, 2, 3, 4, 5\}$ forms a finite abelian group under addition modulo 6.

Drop the element 0 from the set S and form the table for addition modulo 6. Verify that the set does not form a group for want of closure property.

Note. The above set is sometimes written as $S = [\{0, 1, 2, 3, 4, 5\}, +6]$.

26. Form the operation table for the set

$S = \{1, 2, 3, 4, 5\}$ under multiplication modulo 6 and show that the set does not form a group under this operation.

Note. This set is sometimes written as $S = [\{1, 2, 3, 4, 5\}, \times 6]$.

27. Show that the set $S = \{0, 1, 2, 3, 4\}$ forms a group under addition modulo 5 and the set $S = \{1, 2, 3, 4, 5, 6\}$ forms an abelian group under multiplication modulo 7.

28. Show that the set of integers $\{1, 5, 7, 11\}$ forms a group under multiplication modulo 12.

29. Show that the residue classes modulo 4 do not form a group with respect to multiplication of residue classes. Show further that it forms a group with respect to addition of residue classes.

30. Show that the residue classes [1], [3], [5], [7] modulo 8 form a group with respect to multiplication of residue classes.

31. Show that the set $I_n = \{0, 1, 2, \ldots\ldots, (n-1)\}$ of first n non-negative integers forms a group under addition modulo n.

32. Show that, if p be a prime number, then the set

$$I_p = \{1, 2, \ldots\ldots, (p-1)\}$$

forms an abelian group under multiplication modulo p.

33. Show that the residue classes modulo n form a finite group with respect to addition of residue classes.

34. Show that the non-zero residue classes modulo a prime p form a group with multiplication of residue classes.

35. Show that the non-zero residue classes modulo a composite integer n do not form a group under multiplication of residue classes.

3.8. Permutations.

Permutation of a non-empty finite set is defined to be a one-one mapping of a finite set onto itselt (a bijective mapping). Let $a, b, c, \ldots\ldots, k$ be any arrangement of the set of integers $1, 2, 3, \ldots\ldots, n$.

The symbol

$$p = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ a & b & c & \ldots\ldots & k \end{pmatrix}$$

means : replace 1 by a, 2 by b, 3 by c, etc. until finally n is replaced by k, that is, we get a one-one mapping of the finite set $\{1, 2, 3, \ldots\ldots, n\}$ onto itself. Such a symbol denotes *permutation*.

Obviously, the order of the column in the symbol is immaterial so long as the corresponding elements above and below in that column remain unchanged.

The order, in which the first row is written, does not matter ; what actually matters is which element is replaced by which.

Thus $\begin{pmatrix} 1 & 2 & 3 \\ b & a & c \end{pmatrix}, \begin{pmatrix} 3 & 2 & 1 \\ c & a & b \end{pmatrix}$ and $\begin{pmatrix} 2 & 3 & 1 \\ a & c & b \end{pmatrix}$ are the same.

In the standard form, the elements in the top row are in the natural order.

The number of elements of a finite set is the *degree* of the permutation.

Thus permutation p of the set $S = \{1, 2, 3, \ldots\ldots, n\}$ means that by the bijective mapping p, $(a, b, c, \ldots\ldots, k)$ are the images of

$$(1, 2, 3, \ldots\ldots, n).$$

This may also be expressed as

$$p(1) = a,\ p(2) = b,\ p(3) = c, \ldots\ldots, p(n) = k.$$

Thus , if $p : S \to S$ and p be one-one onto, then p is a permutation of degree n.

Two permutations p and q of degree n are said to be *equal*, if we have $p(a) = q(a)$, for all $a \in S$. Thus

$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ and $q = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ are two equal permutations.

If the set contains n elements, then the set of permutations p will contain n ! elements, as n distinct elements can be arranged in n ! ways.

In particular, if $n = 3$, then the elements of this set will be

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

The set of all permutations of a set containing n elements is denoted by P_n. The set P_n will contain n ! distinct elements and is called the symmetric set of permutations.

If there be no change of the elements, that is, if each element be replaced by itself, then it is called the *identity permutation* and is denoted by the symbol I.

Thus $I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$ or $\begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ 1 & 2 & 3 & \ldots\ldots & n \end{pmatrix}$.

The identity mapping is also a bijective mapping.

3.9. Product of permutations.

The product of two permutations p and q of same degree is denoted by $p\,o\,q$ or pq, meaning first perform p and then perform q, that is,

If $p = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$ and $q = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$,

then $p\,o\,q = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} o \begin{pmatrix} a & c & b \\ b & c & a \end{pmatrix}$, order of columns being immaterial ; q has been written in such a way that the first row of q coincides with the second row of p.

Then, by definition, $p\,o\,q = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$.

$p\,o\,q$ is itself a permutation of same degree.

The working formula is thus :

Replace a by a in p, then replace a by b in q ; replace b by c in p, then replace c by c in q ; replace c by b in p, then replace b by a in q, so that the upper line of q is the lower line of p. Thus, finally a changes to b, b changes to c and c changes to a. It is thus to cancel the second row $(a\ c\ b)$ of p with the first row $(a\ c\ b)$ of q.

Note. This is another definition of the product. This definition or that given in Article 1.22 may be used while working out examples.

For any permutation p, it can be easily seen that

$$pI = Ip = p,$$

in which the identity permutation I is of the same degree as p.

In general, multiplication of two permutations is not commutative.

For example, if $p = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ and $q = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, then

as before $pq = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$; but $qp = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

This is true for permutation of any number of elements.

If p and q be two permutations of the same degree and if $pq = qp = I$, where I is the identity permutation of the same degree as p and q, then q is called the *inverse permutation* of p and is denoted by p^{-1}.

Since p is a bijective mapping, it admits of a unique inverse and p^{-1} is also bijective.

For the permutation $p = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ a_1 & a_2 & a_3 & \ldots\ldots & a_n \end{pmatrix}$,

the inverse is $p^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots\ldots & a_n \\ 1 & 2 & 3 & \ldots\ldots & n \end{pmatrix}$ and is a permutation.

It can be easily verified that $pp^{-1} = p^{-1}p = I$, the identity permutation.

Let p be a permutation on a set of degree n. Then we define

$p^n = p.p.p.....p$ (n factors), for all $n \in N$ and

$p^{-n} = p^{-1}.p^{-1}.p^{-1}.....p^{-1}$ (n factors), for all $n \in N$.

Also we define $p^0 = I$.

For all integral values of m and n, we have the index laws

(*i*) $p^m . p^n = p^{m+n}$, (*ii*) $\left(p^m\right)^n = p^{mn}$.

But, as in general, $pq \neq qp$, $(pq)^m = p^m \cdot q^m$ does not hold.

The *order* of a permutation p is the least positive integer n, such that

$p^n =$ the identity permutation I.

3.10. Group property of permutations.

A group, whose elements are permutations, is called a *permutation group.*

If we combine any two permutations by multiplication, then the result is another permutation.

As there are n ! different arrangements for n symbols, there are n ! permutations on n symbols. These can be obtained by inserting the n ! different arrangements of $1, 2, \ldots\ldots, n$ in the second row of p.

Theorem. *The set of n ! permutations on n symbols forms a group with the operation permutation multiplication.*

Let P_n be the set of all n ! permutations of $S = \{1, 2, 3, \ldots\ldots, n\}$.

If we combine any two permutations by multiplication, then the result is another permutation belonging to P_n. Thus the system is closed under permutation multiplication.

Let p, q, r be the three permutations on n symbols as given by

$$p=\begin{pmatrix}1 & 2 & 3 & \ldots\ldots & n\\ a_1 & a_2 & a_3 & \ldots\ldots & a_n\end{pmatrix}, q=\begin{pmatrix}a_1 & a_2 & \ldots\ldots & a_n\\ b_1 & b_2 & \ldots\ldots & b_n\end{pmatrix}, r=\begin{pmatrix}b_1 & b_2 & \ldots\ldots & b_n\\ c_1 & c_2 & \ldots\ldots & c_n\end{pmatrix},$$

where $(a_1, a_2, \ldots\ldots, a_n), (b_1, b_2, \ldots\ldots, b_n)$ and $(c_1, c_2, \ldots\ldots, c_n)$ are any arrangement of the set of integers 1, 2, 3,....., n.

Then $p, q, r \in P_n$.

Now $pq=\begin{pmatrix}1 & 2 & \ldots\ldots & n\\ b_1 & b_2 & \ldots\ldots & b_n\end{pmatrix}$ and $qr=\begin{pmatrix}a_1 & a_2 & \ldots\ldots & a_n\\ c_1 & c_2 & \ldots\ldots & c_n\end{pmatrix}$.

Again

$$(pq)r=\begin{pmatrix}1 & 2 & \ldots\ldots & n\\ c_1 & c_2 & \ldots\ldots & c_n\end{pmatrix} \text{ and } p(qr)=\begin{pmatrix}1 & 2 & \ldots\ldots & n\\ c_1 & c_2 & \ldots\ldots & c_n\end{pmatrix}.$$

Thus $(pq)r = p(qr)$, that is, permutation multiplication is associative.

If $p=\begin{pmatrix}1 & 2 & \ldots\ldots & n\\ a_1 & a_2 & \ldots\ldots & a_n\end{pmatrix}$, then the identity permutation is

$$I=\begin{pmatrix}1 & 2 & \ldots\ldots & n\\ 1 & 2 & \ldots\ldots & n\end{pmatrix}.$$

It is obvious now that $Ip = pI = p$, for all p in P_n.

Thus I is the identity.

It can be easily shown further that $pp^{-1} = p^{-1}p = I$, where

$p^{-1}=\begin{pmatrix}a_1 & a_2 & \ldots\ldots & a_n\\ 1 & 2 & \ldots\ldots & n\end{pmatrix}$ from the definition of p^{-1}.

Thus p^{-1} is the inverse of the element p and $p^{-1} \in P_n$.

Thus the $n!$ permutations of the set P_n on n symbols form a group with respect to permutation multiplication, as it satisfies all the group axioms.

Permutation multiplications being, in general, not commutative, $P_n (n > 2)$ forms a finite non-abelian group.

This group is called a *symmetric permutation group* on n-symbols and is denoted sometimes by S_n.

Notice that S_1 and S_2 are abelian.

3.11. Cyclic permutations.

Some permutations are written in cyclic forms. For example, the permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad \ldots (1)$$

may be written simply as (1 2 4 3), which means : 1 is replaced by 2, 2 is replaced by 4, 4 is replaced by 3, and 3 is replaced by 1.

Such a permutation is called a *cycle.*

A permutation which replaces n objects cyclically is called a *cyclic* (or *circular*) *permutation* of degree n.

We can write $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ 2\ 3\ 4)$.

The meaning of this symbol is to replace each number which follows and the last number by the first. We can change the places of the elements without changing the cyclic order. Thus

$$(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3).$$

Thus a circular permutation may be denoted by more than one one-rowed symbols.

The number of symbols permuted by a cycle is called its *length.* In general, if r symbols be permuted in a permutation, then it is said to be a *cycle of length* r or *r-cycle.*

The permutation

$$q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

is written as the cycle (3 4 5) and means : 1 and 2, the missing symbols in (3 4 5), are replaced by themselves and 3 is replaced by 4, 4 is replaced by 5 and 5 is replaced by 3.

q is also written as (1) (2) (3 4 5).

The cycles (1) and (2) are each of length 1 and the cycle (3 4 5) is of length 3.

If a cycle consists of a single element, then that element is often omitted from the symbol of permutation. Thus

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} = (1\ 2\ 3\ 4)(5) = (1\ 2\ 3\ 4).$$

Again $r = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$

is written as (2 3) (4 5) or (1) (2 3) (4 5). Here 1 remains unchanged, 2 is replaced by 3 and 3 is replaced by 2 ; 4 is replaced by 5 and 5 is replaced by 4. (2 3) (4 5) is called the *product of the cycles*. These cycles are *disjoint* – none of them having a symbol in common. (1 3 4) and (2 5) are disjoint but (1 3 4) and (2 3 5) are not.

Let us consider the product of the disjoint cycles (1 2 3) and (4 5).

$$(1\,2\,3)(4\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 2 & 3 & 1 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \quad \ldots \quad (2)$$

and the product is a permutation.

Similarly, $(1\,2\,3)\,(5\,6\,7\,8) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 6 & 7 & 8 & 5 \end{pmatrix}$.

From (1) and (2), we conclude that *every permutation of a finite set is either a cycle or a product of disjoint cycles.*

Note 1. The identity permutation $I = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ 1 & 2 & 3 & \ldots\ldots & n \end{pmatrix}$ is the product of n disjoint cycles (1), (2),....., (n) each of length 1.

Note 2. It can be easily verified that the product of disjoint cycles is commutative.

3.12. Transpositions.

A permutation that displaces only two symbols is called a *transposition.* Thus transposition is a cycle of length two.

Theorem 1. *Every permutation of a finite set containing at least two elements can be expressed as a finite product of transpositions.*

Consider the product of two transpositions

$$(1\,2)(1\,3) = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ 2 & 1 & 3 & \ldots\ldots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ 3 & 2 & 1 & \ldots\ldots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & n \\ 2 & 3 & 1 & \ldots\ldots & n \end{pmatrix} = (1\,2\,3).$$

Thus (1 2) (1 3) = (1 2 3).

Again (1 2) (1 3) (1 4) = (1 2 3) (1 4)

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots\ldots & n \\ 2 & 3 & 1 & 4 & \ldots\ldots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots\ldots & n \\ 4 & 2 & 3 & 1 & \ldots\ldots & n \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots\ldots & n \\ 2 & 3 & 4 & 1 & \ldots\ldots & n \end{pmatrix} = (1234).$$

Thus (1 2) (1 3) (1 4) = (1 2 3 4).

In general, if we assume

$$(1\,2)(1\,3)(1\,4)\ldots\ldots(1\,m) = (1\,2\,3\,4\,\ldots\ldots\,m),$$

then $(1\,2\,3\,4\ldots\ldots m)\,(1\,m+1) = \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & m & m+1 \\ 2 & 3 & 4 & \ldots\ldots & 1 & m+1 \end{pmatrix}$

$$\times \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & m+1 \\ m+1 & 2 & 3 & \ldots\ldots & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & \ldots\ldots & m & m+1 \\ 2 & 3 & 4 & \ldots\ldots & m+1 & 1 \end{pmatrix}$$

$$= (1\,2\,3\ldots\ldots m\ m{+}1).$$

Thus we have

$(1\,2\,3\ldots\ldots m\ m{+}1) = (1\,2)\,(1\,3)\ldots\ldots\,(1\,m)\,(1\ m{+}1).$

Writing $n = m+1$, we have the theorem

$$(1\,2\,3\,\ldots\ldots\,n) = (1\,2)\ (1\,3)\ \ldots\ldots\ (1\,n),$$

as it is seen to be true for $n = 2, 3, 4$ and by induction, $n = m$.

Thus *a cycle of n symbols can be written as a product of* $(n-1)$ *transpositions.*

We know that a permutation can be expressed as the product of disjoint cycles. Hence the theorem follows.

Theorem 2. *A permutation when expressed as a product of transpositions, the number of transpositions is either always even or always odd.*

Let $x_1, x_2, \ldots\ldots, x_n$ be the n distinct symbols and consider the alternating function F, which is the product of $\frac{n(n-1)}{2}$ factors of the form $(x_i - x_j)$, $i < j$, where $i, j = 1, 2, \ldots\ldots, n$.

Thus $F=(x_1-x_2)(x_1-x_3)(x_1-x_4).....(x_1-x_n)$

$(x_2-x_3)(x_2-x_4).....(x_2-x_n)$

$(x_3-x_4).....(x_3-x_n)$

.....

$(x_{n-1}-x_n)$.

Let us operate F by the transposition $f=(x_i,x_j)$, where $i<j$.

The factors of F which contain neither x_i nor x_j remain unchanged when F is operated by f, while the factor (x_i-x_j) of F, being operated by the permutation f, changes sign and becomes $-(x_i-x_j)$.

The factors of F which contain either x_i or x_j only may be grouped into pairs of products

$$\pm(x_m-x_i)(x_m-x_j), \text{ where } m\neq i, j.$$

These products remain unchanged when operated by the permutation f.

Thus F becomes $(-F)$ when operated by a transposition f.

Now, let p be a permutation which can be written as a product of a transpositions and also as a product of b transpositions. When F is operated by p we shall thus obtain $(-1)^a F$, as p is a product of a transpositions ; we shall also obtain $(-1)^b F$, as p is a product of b transpositions too. But, p being the same permutation, no matter how we write it, we must have

$$(-1)^a F=(-1)^b F.$$

Therefore $a\equiv b \pmod 2$.

Thus a permutation cannot be both even and odd.

Hence the theorem follows.

Theorem 3. *The order of an r-cycle is r.*

Let $(1, 2, 3,....., r)$ be an r-cycle of the permutation

$$p=\begin{pmatrix}1&2&3&.....&r&r+1&.....&n\\2&3&4&.....&1&r+1&.....&n\end{pmatrix} \text{ of a finite set}$$

$$S=\{1,2,.....,n\}.$$

Then we have $p(1)=2,\ p^2(1)=p(2)=3,.....,\ p^r(1)=1$.

Similarly, $p(2)=3$, $p^2(2)=p(3)=4,\ldots\ldots$, $p^{r-1}(2)=1$,

$p^r(2)=p(1)=2$ and so on. Thus

$$p^r(1)=1,\ p^r(2)=2,\ldots\ldots,p^r(r)=r\ . \qquad \ldots\ (1)$$

Again we have $p(r+1)=r+1,\ldots\ldots,p(n)=n$.

Therefore $p^r(r+1)=r+1,\ldots\ldots,p^r(n)=n$. $\qquad \ldots\ (2)$

From (1) and (2), we have $p^r(k)=k$, for $k=1, 2,\ldots\ldots,n$, so that p^r is an identity permutation.

r is the least positive integer for which $p^r=I$, the identity permutation.

Hence the order of p is r.

On the contrary, if there be any positive integer $m<r$, then $p^m(1)$ would have been equal to 1, which is not the case.Hence the theorem follows.

Theorem 4. *The order of a permutation of a finite set is the L.C.M. of the lengths of its disjoint cycles.*

Let p be a permutation on the finite set $S=\{1, 2,\ldots\ldots, n\}$. We further assume that p can be expressed as a product of m disjoint cycles $f_1, f_2,\ldots\ldots,f_m$ of lengths $r_1, r_2,\ldots\ldots,r_m$, so that

$$p=f_1 f_2 \ldots\ldots f_m\ .$$

Since multiplication of disjoint cycles is commutative, we have, for a positive integer n,

$$p^n=f_1^{\,n} f_2^{\,n} \ldots\ldots f_m^{\,n}\ .$$

Now we know that, if I be the identity permutation, then

$$f_1^{r_1}=f_2^{r_2}=\cdots\cdots=f_m^{r_m}=I\ .$$

Let s be the common multiple of $r_1, r_2,\ldots\ldots,r_m$.

Then we have $p^s=f_1^{\,s} f_2^{\,s}\ldots\ldots f_m^{\,s}=I$.

Obviously, the least positive integer r, for which $p^r=I$ holds, must be the least value of s, that is to say, r is the L.C.M. of

$$r_1, r_2,\ldots\ldots,r_m\ .$$

Hence the order of p is the L.C.M. of the lengths $r_1, r_2,\ldots\ldots,r_m$.

3.13. Even and odd permutations.

A permutation is called an *even* permutation or an *odd* permutation according as it can be written as a product of an even number or an odd number of transpositions.

Thus the permutation α given by $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 4 & 1 & 3 \end{pmatrix}$ is odd, because $\alpha = (1\ 5)(2\ 6\ 3) = (1\ 5)(2\ 6)(2\ 3)$.

Again the permutation β as given by $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is even, because $\beta = (1\ 6)(2\ 3\ 4\ 5) = (1\ 6)(2\ 3)(2\ 4)(2\ 5)$.

By convention, the sign of a permutation is taken to be positive or negative according as the permutation is even or odd.

It can be easily verified that the product of two permutations is an even permutation if either both the permutations be odd or both be even. But, if one permutation be odd and the other be even, then the product becomes odd.

Inverse of a permutation, even or odd, maintains its own nature (that is, remains even or odd).

Note. A cycle containing an odd number of symbols is an even permutation, whereas a cycle containing an even number of symbols is an odd permutation.

Theorem. *Of the n! permutations on n symbols* $(n>1)$, $\frac{n!}{2}$ *are even permutations and* $\frac{n!}{2}$ *are odd permutations.*

Of the n ! permutations on n symbols, let the even permutations be $e_1, e_2, \ldots\ldots, e_m$ and the odd permutations be $o_1, o_2, \ldots\ldots, o_k$, so that $m+k = n$!.

Multiply each of these permutations on the left by a transposition t which is of course an odd permutation.

Thus $te_1, te_2, \ldots\ldots, te_m$ are all odd permutations and $to_1, to_2, \ldots\ldots, to_k$ are all even permutations.

Now an odd permutation is never equal to an even permutation, that is, $te_i \neq to_j$ for any $i = 1, 2, \ldots\ldots, m$; $j = 1, 2, \ldots\ldots, k$.

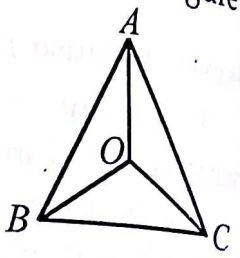
As $e_1, e_2, \ldots\ldots, e_m$ are all distinct, we can say that $te_1, te_2, \ldots\ldots, te_m$ are all distinct; for, the equality of any two of the latter set will imply the equality of the corresponding two elements of the former set by the cancellation law. Similarly, we say that $to_1, to_2, \ldots\ldots, to_k$ are all distinct elements.

Thus the m odd permutations $te_1, te_2, \ldots\ldots, te_m$ are simply the odd permutations $o_1, o_2, \ldots\ldots, o_k$ in some order and the even k permutations $to_1, to_2, \ldots\ldots, to_k$ are simply the even permutations $e_1, e_2, \ldots\ldots, e_m$ in some order. Again, as $m+k = n$!, therefore $m = k = \frac{n!}{2}$.

3.14. Symmetries of a geometrical figure and dihedral groups.

Let S be the set of all points in a Euclidean space. A symmetry of a geometrical figure, such as an equilateral triangle, a square, a regular pentagon, in the space, is a bijection of S onto S that preserves distance between two points in S and keeps the figure unchanged as a whole.

Let ABC be an equilateral triangle with its centroid at O. Rotating the triangle in the plane about O through angles $0, \frac{2}{3}\pi, \frac{4}{3}\pi$,



we get its respective three transformations, which correspond to the following three permutations of the vertices A, B, C of the triangle :

$$i = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}, \quad r_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}, \quad r_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

since rotation through zero angle corresponds to its original position.

Again, reflecting the triangle about AO, BO and CO, we get another three transformations, which correspond to the following three permutations of the vertices respectively :

$$a = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}, \quad b = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}, \quad c = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.$$

Thus there are six symmetries of the equilateral triangle.

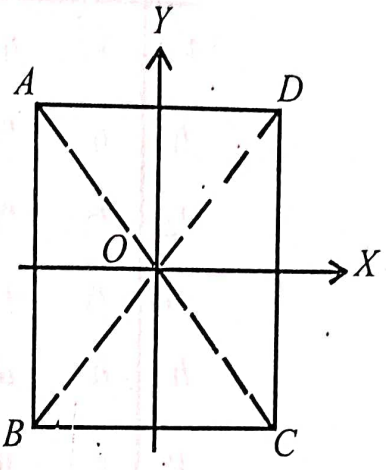
Let $*$ be a binary composition on $S = \{i, r_1, r_2, a, b, c\}$ such that $r_1 * r_1 = r_2$, $r_1 * r_2 = i$, $r_2 * r_2 = r_1$, $a * b = r_1$, $b * a = r_2$, $b * c = r_1$,.....

Then the composition table is given as under.

$*$	i	r_1	r_2	a	b	c
i	i	r_1	r_2	a	b	c
r_1	r_1	r_2	i	c	a	b
r_2	r_2	i	r_1	b	c	a
a	a	b	c	i	r_1	r_2
b	b	c	a	r_2	i	r_1
c	c	a	b	r_1	r_2	i

The group formed by these six symmetries of the triangle is called the *dihedral group* D_3 of order 6. It is a group of symmetry and is a non-commutative group. It is the same as the symmetric group S_3.

Let $ABCD$ be a square with its centre at the origin O and the sides parallel to the co-ordinate axes. Rotating the square in the plane about O through angles $0°$, $90°$, $180°$ and $270°$, we get its respective four transformations i, r_1, r_2, r_3 given by the following four permutations of the vertices A, B, C, D of the square :



$$i = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \quad r_1 = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}, \quad r_2 = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix},$$

$$r_3 = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix},$$

since rotation through $0°$ corresponds to its original position.

Again, rotating the square out of the plane about the horizonal line (that is, the x-axis), the vertical line (that is, the y-axis), the diagonal OA (that is, the line $y = -x$) and the diagonal OB (that is, the line $y = x$), we get another four transformations h, v, d_1, d_2 respectively, which are given by the following permutations of the vertices :

$$h = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \quad v = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix},$$

$$d_1 = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix}, \quad d_2 = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix}.$$

Thus there are eight symmetries of the square.

Let $S = \{i, r_1, r_2, r_3, h, v, d_1, d_2\}$ be the set of the symmetries of the square.

Also let $*$ be a binary composition on the set S as per the composition table given below :

$*$	i	r_1	r_2	r_3	h	v	d_1	d_2
i	i	r_1	r_2	r_3	h	v	d_1	d_2
r_1	r_1	r_2	r_3	i	d_2	d_1	h	v
r_2	r_2	r_3	i	r_1	v	h	d_2	d_1
r_3	r_3	i	r_1	r_2	d_1	d_2	v	h
h	h	d_1	v	d_2	i	r_2	r_1	r_3
v	v	d_2	h	d_1	r_2	i	r_3	r_1
d_1	d_1	v	d_2	h	r_3	r_1	i	r_2
d_2	d_2	h	d_1	v	r_1	r_3	r_2	i

The group formed by these eight symmetries of the square is called the *dihedral group* D_4 of order 8. It is also called the *octive group.*

It is clear that $\{S, *\}$ is a non-commutative group of order 8, i being the identity of the binary operation. Each element except r_1 and r_3, of the group is its own inverse, where $(r_1)^{-1} = r_3$, $(r_3)^{-1} = r_1$:

The symmetries of a regular pentagon form a non-commutative group which is called the *dihedral group* D_5 of order 10.

The symmetries of a regular polygon of n sides form the dihedral group D_n of order $2n$.

3.15. Illustrative Examples.

Ex. 1. *If* $A = (1\,2\,3\,4\,5)$, $B = (2\,3)\,(4\,5)$, *then show that*

$$AB = (1\,3\,5).$$

We have $AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = (1\ 3\ 5).$$

Ex. 2. *Find the inverse of the permutation* $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$.

Let the inverse of the permutation $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$ be $\begin{pmatrix}1&2&3&4\\x&y&u&v\end{pmatrix}$.

Then $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\x&y&u&v\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$,

that is, $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\begin{pmatrix}1&3&4&2\\x&u&v&y\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$

or, $\begin{pmatrix}1&2&3&4\\x&u&v&y\end{pmatrix}=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$.

Therefore $x=1$, $u=2$, $v=3$ and $y=4$.

Hence the inverse is $\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}$.

Note. p^{-1} is obtained just by interchanging the rows of p and then by expressing it in the standard form by interchanging the columns.

Ex. 3. *Show that the permutation* $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ *is even, while the permutation* $\begin{pmatrix}3&4&5&6\\4&5&6&3\end{pmatrix}$ *is odd.* [*T.H. 2009*]

We have $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(1\,2\,3)=(1\,2)(1\,3)$.

Thus the given permutation can be expressed as the product of an even number of transpositions and hence the permutation is even.

Again $\begin{pmatrix}3&4&5&6\\4&5&6&3\end{pmatrix}=(3\,4\,5\,6)=(3\,4)(3\,5)(3\,6)$.

Hence this, being a product of an odd number of transpositions, is an odd permutation.

Ex. 4. *Express the permutation* $\begin{pmatrix}1&2&3&4&5&6\\6&5&2&1&3&4\end{pmatrix}$ *as a product of transpositions. Find also the order of the permutation.*

The given permutation is

$(1\,6\,4)\,(2\,5\,3)$, two disjoint cycles of length 3

$=(1\,6)\,(1\,4)\,(2\,5)\,(2\,3)$.

This is the required product.

The L.C.M. of the lengths of the two disjoint cycles being 3, the order of the permutation is 3.

Examples III (B)

1. Show that $(1\,2\,3)\ (5\,6\,4\,1) = (1\,2\,3\,5\,6\,4)$.

2. If $*$ denotes permutation multiplication, then show that

(*a*) $(2\,3)*(1\,3)\,(2\,4\,5) = (1\,3\,4\ 5\,2)$.

(*b*) $(1\,3)\,(2\,4\,5)*(2\,3) = (1\,2\,4\ 5\,3)$.

(*c*) $(1\,2\,3)*(2\,4\,3)*(1\,3\,4) = (1) = e$.

(*d*) $(1\,2)*(3\,4)*(2\,4) = (1\,4\,3\ 2)$.

3. (*a*) Show that the inverse of the permutation

(*i*) $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ is $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$. (*ii*) $\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$ is $\begin{pmatrix}1&2&3&4&5\\3&1&2&5&4\end{pmatrix}$.

(*b*) Show that the inverse of (1 3) (2 4 5) is (1 3) (2 5 4) and that of the product (1 2 4 5 3) (3 2 1 5 4) is (2 3 5).

(*c*) Show that the inverse of the permutation $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ is itself.

(*d*) $f = (1\,4\,5\,6)$ and $g = (2\,3\,7)$ are two disjoint cycles of seven symbols. Show that $fg = gf$.

4. Show that (*i*) $(2\,3\,4\,5) = (2\,5)\,(3\,4)\,(3\,5)$.

(*ii*) $(1\,4\,3\,2)\,(2\,4\,1)\,(1\,3\,5) = (1\,3\,4\,5)\,(2)$.

5. Show that $(1\,2\,3)\,(4\,5) = (4\,5)\,(1\,2\,3)$

but $(1\,2\,3)\,(2\,3) \neq (2\,3)\,(1\,2\,3)$.

6. (*a*) Express the permutation given below as a product of transpositions and hence find whether it is odd or even :

$$\begin{pmatrix}1&2&3&4&5&6\\5&4&2&6&1&3\end{pmatrix}$$

(*b*) Write down the permutation

$$\begin{pmatrix}1&2&3&4&5&6&7\\5&7&6&2&1&3&4\end{pmatrix}$$

as a product of disjoint cycles and then express it as a product of transpositions.

7. Show that $\begin{pmatrix}1&2&3&4&5&6\\4&3&1&2&6&5\end{pmatrix}$ is an even permutation, while

$\begin{pmatrix}1&2&3&4&5&6&7\\4&3&1&2&6&7&5\end{pmatrix}$ is an odd permutation.

8. (*a*) Show that (6 5 4 3 1 2) is an even permutation while (6 7 5 4 1 2 3) is an odd permutation.

(*b*) Show that the product of two permutations is an even permutation if either both the permutations are even or both odd and the product is an odd permutation if one permutation is odd and the other even.

9. (*a*) Show that identity permutation is an even permutation.

(*b*) Show that the inverse of an even permutation is an even permutation and the inverse of an odd permutation is an odd permutation.

10.(*a*) Show that if the permutation $\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}$ be multiplied three times to itself, then it will give an identity permutation.

(*b*) If $p = (1\,2\,3\,4\,5)$, then show that $p^5 = I$.

11. For two permutations $A=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ and $B=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, show that $AB = BA = I$.

12. Show that the inverse of the permutation (3 4) of degree four is (4 3).

13. If $x = (1\,2\,3)$, $y = (2\,4\,3)$ and $z = (1\,3\,4)$, then show that $xyz = 1$.

14.(*a*) Prove that the set S_3 consisting of three permutations I, $(a\,b\,c)$, $(a\,c\,b)$ on three symbols a, b, c forms a finite abelian group with respect to permutation multiplication.

[Let $I = a_1, (abc) = a_2, (acb) = a_3$. To get the element at the intersection of second row and third column of the composition table, compute $a_2 * a_3$ and so on]

(*b*) Show that S_4 is a non-abelian group. [*B.H. 2001*]

(*c*) In a symmetric group S_4 of degree 4, solve the equation

$$x \circ (1\,2\,3) = (2\,4\,3).$$ [*C.H. 1996*]

15. Prove that $(a_1\, a_2 \ldots\ldots a_n)^{-1} = (a_n\, a_{n-1} \ldots\ldots a_1)$.

16. Verify the group properties by taking the set of all permutations of the elements 1, 2, 3. Show further that the symmetric group S on $\{1, 2, 3\}$ is non-commutative.

17. If $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, then show that $A^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$.

Show also that the order of A is 4.

18. Show that the order of the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$ is six.

19. Find the images of the elements 3 and 4, if

(*i*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & & & 4 \end{pmatrix}$ be an odd permutation;

(*ii*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & & & 1 & 4 \end{pmatrix}$ be an even permutation.

20. If $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, then show that

$$(fg)^{-1} = g^{-1}f^{-1}.$$ [*B.H. 1998*]

Answers

6. (*a*) (1 5), (2 4), (2 6), (2 3); even.

(*b*) (1 5), (2 7 4), (3 6); (1 5), (2 7), (2 4), (3 6). **14.** (*c*) $x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$.

19. (*i*) 1, 5. (*ii*) 5, 6.

3.16. Order of an element of a group.

Let $(G, \bullet)$ be a group and $a \in G$. We define

a^1 by a, a^2 by $a.a$, a^3 by $a.(a.a) = (a.a).a = a.a.a$.

In the same way, we define a^m, where m is a positive integer. The product is independent of the manner in which the factors are grouped.

If m be a negative integer, say $m = -p$, where p is a positive integer, then we define a^m by $(a^{-1})^p$.

In addition operation, we write $ma = a + a + \ldots\ldots + a$ (m terms).

For a^0, we define it to be the identity element of the group for multiplication and $0a = 0$ for addition.

It can be shown that if $a \in G$ in the group $(G, *)$, then

(i) $a^{m+n} = a^m * a^n$; (ii) $(a^m)^n = a^{mn}$; (iii) $(a^n)^{-1} = a^{-n}$

for all integral values of m and n.

Again $(a^m)^{-1} = (a.\ a.\ a.....m \text{ factors})^{-1} = a^{-1}.\ a^{-1}.\ a^{-1}..... m \text{ factors}$

$= (a^{-1})^m$.

For addition, we have $na = -(ma) = m(-a)$, if $n = -m$.

The *order* of an element a of a group G is the least positive integer n, such that $a^n = e$ (the identity element of G).

The order of the element (–1) of the multiplicative group {–1, 1} is 2, since $(-1)^2 = 1$, which is the identity element of the group.

If there exists no such integers as n, we say that a is of *infinite* or of *zero order*.

The symbol $o(a)$ is used to denote the order of a.

In the group $(a, a^2, a^3, a^4, a^5, a^6 = e)$, we have

$o(a^2) = 3$, since $(a^2)^3 = e$; $o(a^4) = 3$, since $(a^4)^3 = e$;

$o(a^5) = 6$, since $(a^5)^6 = a^{30} = (a^6)^5 = e^5 = e$.

Consider the multiplicative group $\{1, -1, i, -i\}$ in which the identity element is 1. Now the order of (–1) is 2, since 2 is the least positive integer such that $(-1)^2 = 1$. The order of i is 4, as $(i)^4 = 1$. The order of $(-i)$ is similarly 4. The order of the identity element only is 1.

In an infinite multiplicative group of non-zero rational numbers, the order of every element, except the elements 1 and (–1), is infinite ; for, we have the order of (–1) as 2, but there being no such positive n so that $2^n = 1$, the identity element, the order of 2 is infinite.

For the group $(Z, +)$, 0 is the identity element. We can show that the order of every element except zero is infinite, since there is no n such that n (integer other than 0) = 0.

3.17. Theorems on the order of an element of a group.

Theorem 1. *The order of every element of a finite group is finite and is less than or equal to the order of the group.*

Let a be an element of the finite group G. Let us consider all positive integral powers of a, namely

$a, a^2, a^3, a^4, ...$

Every one of these powers must belong to G. But as G is finite, all these elements cannot be different. Let us suppose

$$a^s = a^r, s > r.$$

This implies that $a^s a^{-r} = a^r . a^{-r}$,

that is, $a^{s-r} = a^0 = e$.

Therefore $a^t = e$, putting $s - r = t > 0$.

Thus there is a positive integer t for which $a^t = e$.

Now every set of positive integers has a least number. Hence the set of all those positive integers t such that $a^t = e$ has a least number, say p. Thus there exists a least positive integer p such that $a^p = e$. This shows that the order of every element of a finite group is finite.

If possible, let $o(a) = n > o(G)$. Suppose $a \in G$; then, by closure property, $a, a^2, ..., a^n$ are elements of G and no two of these elements are equal. For, if possible, let

$$a^r = a^s, 1 \le s < r \le n.$$

Then $a^{r-s} = e$.

Since $0 < r - s < n$, $a^{r-s} = e$ implies that the order of a is less than n which is a contradiction. Hence $a, a^2, ..., a^n$ are the n distinct elements of G.

Since $n > o(G)$, this is not possible and hence

$$o(a) \le o(G).$$

This shows that the order of an element cannot exceed the order of the group.

Theorem 2. *The order of any integral power of an element a cannot be greater than that of a.*

Let a^k be any power of a. Let n and m be the orders of a and a^k respectively.

Then $a^n = e$ and $(a^k)^m = e$.

Now $(a^k)^n = (a^n)^k = e^k = e$.

But m is the least positive integer, such that $(a^k)^m = e$. Therefore $m \le n$, which shows that the order of a^k cannot exceed the order of a.

Theorem 3. *The order of an element of a group is the same as that of its inverse.*

Let n and m be the orders of a and its inverse a^{-1} respectively.

Therefore $a^n = e$ and $\left(a^{-1}\right)^m = e$.

Since a^{-1} is a power of a, by the previous theorem, we must have

$$m \le n. \quad \ldots (1)$$

Again $\left(a^{-1}\right)^m = e$ implies $a^{-m} = e$,

that is, $a^{-m}a = ea$, whence $a^{-(m-1)} = a$.

This gives $\left(a^{-1}\right)^{(m-1)} = a$.

Thus a is a power of a^{-1}.

Hence, by the previous theorem, $o(a) \le o\left(a^{-1}\right)$

that is, $n \le m$. $\ldots (2)$

From (1) and (2), it is clear that $m = n$.

Theorem 4. *The orders of the elements a and $x^{-1}ax$ are the same, where a and x are two elements of the group.*

Let $o(a) = n$; then $a^n = e$.

Now $\left(x^{-1}ax\right)^2 = \left(x^{-1}ax\right)\left(x^{-1}ax\right)$

$= x^{-1}a\left(xx^{-1}\right)ax$

$= x^{-1}aeax$

$= x^{-1}a^2x$.

In general, $\left(x^{-1}ax\right)^n = x^{-1}a^nx$

$= x^{-1}ex$, since $a^n = e$

$= x^{-1}x = e$.

Again, since $a^m \ne e$ for $0 < m < n$, $\left(x^{-1}ax\right)^m \ne e$.

Thus n is the least positive integer, for which

$$\left(x^{-1}ax\right)^n = e.$$

Hence $o\left(x^{-1}ax\right) = o(a)$.

Cor. If a and b be the arbitrary elements of a group, then

$$o(ab) = o(ba);$$

for, $a^{-1}(ab)a = \left(a^{-1}a\right)(ba) = e(ba) = ba$.

Hence $o(ab) = o\left\{a^{-1}(ab)a\right\}$.

Therefore $o(ab) = o(ba)$.

Thus ab and ba have the same order.

Theorem 5. *If the element a of a group G be of order n, then $a^m = e$, if and only if $m = nq$, m and q being integers.*

Let $a^m = e$. Now, if n be the least positive integer such that $a^n = e$, then we have $m > n$.

Then $m = nq + r$, $0 \le r < n$.

Hence $a^m = e$ implies $a^{nq+r} = e$, that is, $a^{nq} \cdot a^r = e$.

Therefore $(a^n)^q a^r = e$, giving $a^r = e$, since $a^n = e$.

But this is not possible, since $r < n$ and the order of a is n.

Hence $r = 0$ and $m = nq$.

Conversely, let $m = nq$.

Then $a^m = a^{nq} = (a^n)^q = e$. Hence $a^m = e$.

This can be stated as follows :

Let a be an element of a group and let $o(a) = n$. If m be an integer, then $a^m = e$ iff $m \equiv 0 \pmod{n}$.

Theorem 6. *If a be an element of order n in a group and p be prime to n, then a^p is also of order n.*

Let m be the order of a^p.

Now $o(a) = n \Rightarrow a^n = e$ (identity)

$$\Rightarrow (a^n)^p = e^p = e$$

$$\Rightarrow (a^p)^n = e$$

$$\Rightarrow o(a^p) \le n \text{, by theorem 2}$$

that is, $m \le n$, ... (1)

Since p and n are relatively prime, there exist integers x and y such that

$$px + ny = 1.$$

Therefore $a = a^1 = a^{px+ny} = a^{px} \cdot a^{ny}$

$$= a^{px} \cdot (a^n)^y = a^{px} \cdot e^y$$

$$= a^{px} \cdot e = a^{px} = (a^p)^x.$$

Now $a^m = \left[\left(a^p\right)^\lambda\right]^m = \left(a^p\right)^{m\lambda} = \left[\left(a^p\right)^m\right]^\lambda$

$= e^\lambda$, since $o\left(a^p\right) = m$

$= e$.

Hence $o(a) \le m \Rightarrow n \le m$. ... (2)

From (1) and (2), we have $m = n$.

3.18. Sub-group and alternating group.

If we consider two groups, one composed of a set S and the operation $*$ and the other composed of a non-empty set H and the same operation $*$, then we say that the latter is a *sub-group* of the former group, if $H \subset S$.

In other words, a sub-set of elements of a group $(G, *)$, that is, itself a group under $*$ is called a sub-group of G.

If H be a sub-group of G and K be a sub-group of H, then K is a sub-group of G.

Thus every group G has at least two sub-groups, one is the identity group, consisting of the identity element only and the other is the group G itself. These two are called *improper* or *trivial* sub-groups ; others are called *proper sub-groups*.

Q^* is a proper sub-group of R^* under multiplication.

$Q^* \subset Q$, but $(Q^*, \cdot)$ is not a sub-group of $(Q^*, +)$ as the operation in the sub-set Q^* is different from that of Q.

The multiplicative group $\{1, -1\}$ is a proper sub-group of the multiplicative group $\{1, -1, i, -i\}$.

Example of a sub-group is the additive group of integers which is a sub-group of the additive group of rational numbers.

The additive group of rational numbers is again a sub-group of that of real numbers.

The multiplicative group of positive real numbers is a sub-group of the multiplicative group of all non-zero real numbers.

The multiplicative group of non-zero rationals is a sub-group of that of non-zero reals.

On the other hand, the compositions being different, the multiplicative group of positive real numbers is not a sub-group of the additive group of all real numbers.

A *complex* is any non-empty sub-set of a group, whether it is a sub-group or not.

The group of the even permutations from S_n is called the *alternating group* on $\{1, 2, 3, \ldots\ldots, n\}$ of degree n and is denoted by A_n.

We know that the product of two even permutations is an even permutation. Now, if we consider the sub-set of all even permutations (of $\frac{n!}{2}$ elements) of the set of all permutations of n elements, then we see that it is associative with respect to multiplication, as it is a sub-set of the symmetric set S_n. Furthermore, this sub-set possesses identity element and inverses. Thus the sub-set of the even permutations of the symmetric set S_n is a finite group of order $\frac{n!}{2}$ with respect to multiplication. Hence it is a sub-group of S_n.

The set of even permutations of the symmetric group S_3 is an alternating group.

The *centre* of a group $(G, *)$ is the sub-set of elements in G that commute with every element of G and is denoted by $Z(G)$.

Thus $Z(G) = \{x \in G : x * g = g * x \text{ for all } g \text{ in } G\}$.

The centre $Z(G)$ *is a sub-group of* G.

To prove this, we proceed as follows :

In a group G, $e * x = x = x * e$, for all x in G.

Thus $e \in Z(G)$ and hence $Z(G)$ is non-empty.

Let $a, b \in Z(G)$. Then $a * x = x * a$, $b * x = x * b$ for all x in G.

Now

$$(a * b) * x = a * (b * x) = a * (x * b) = (a * x) * b = (x * a) * b = x * (a * b).$$

Hence $a * b \in Z(G)$ for all $a, b \in Z(G)$.

Again let $a \in Z(G)$. Then $a * x = x * a$ for all $x \in G$.

Hence $a^{-1} * (a * x) * a^{-1} = a^{-1} * (x * a) * a^{-1}$

$$\Rightarrow x * a^{-1} = a^{-1} * x \text{ for all } x \in G.$$

Thus $a \in Z(G)$ implies $a^{-1} \in Z(G)$.

All the properties are conserved in $(Z(G), *)$.

Hence $Z(G)$ is a sub-group of $(G, *)$.

$Z(G)$ is a commutative sub-group of G. If G be a commutative group, then $Z(G) = G$ and conversely, if $Z(G) = G$, then G is a commutative group.

If a be a fixed element of a group $(G, *)$, then the *centralizer* of a in G is the set of all elements in G that commute with a and is denoted by $C(a)$. Thus $C(a) = \{x \in G : a * x = x * a\}$.

The centralizer $C(a)$ is a sub-group of G.

To prove this, we proceed similarly as in the case of the centre $Z(G)$.

Theorem 1. *The identity of a sub-group is the same as that of the group.*

Let H be the sub-group of the group G for certain operation and let e and e' be the identity elements of G and H respectively.

Now, if $a \in H$, then $a \in G$ and $ae = a$, since e is the identity of G.

Also $a \in H$.

Therefore $ae' = a$, since e' is the identity element of H.

Thus $ae = ae'$, which gives $e = e'$.

Hence the theorem follows.

Theorem 2. *The inverse of any element of a sub-group is the same as the inverse of the same element regarded as an element of the group.*

Let H be the sub-group of the group G for certain operation and let e be their common identity element.

If $a \in H$, then $a \in G$.

Let b be the inverse of $a \in H$

and c be the inverse of $a \in G$.

Then $ab = e$, since b is the inverse of $a \in H$

and $ac = e$, since c is the inverse of $a \in G$.

Therefore $ab = ac$, which gives $b = c$.

Hence the theorem follows.

Note. Since the identity of H is the same as that of G, the order of an element of H is the same as the order of that element regarded as a member of G.

Theorem 3. *The necessary and sufficient conditions that a non-empty sub-set S of a group G forms a sub-group under the binary operation $*$ in G are*

(i) $a \in S$, $b \in S$ *implies* $a * b \in S$;

(ii) $a \in S$ *implies* $a^{-1} \in S$, *where* a^{-1} *is the inverse of a in G.*

We are given that the sub-set S forms a group under the binary operation $*$ in G.

Since S is a group and $a, b \in S$,

therefore $a * b \in S$.

If e be the identity element of G, then it is also the identity element of S.

In a group, the identity element being unique, e is the unique identity element in S.

Again, let a^{-1} be the inverse of a in G, where $a \in S$.

Therefore $a^{-1} * a = e \in S$.

Now, in a group, every element has unique inverse and S being a group, the inverse of a must be unique in S.

Thus $a \in S$ implies $a^{-1} \in S$.

Hence, if S be a sub-group, then

$a \in S, b \in S$ imply $a * b \in S$

and $a \in S$ implies $a^{-1} \in S$.

Thus the conditions are *necessary*.

To prove that these conditions are also *sufficient*, we observe from the given conditions that the binary operation $*$ in G is also a binary operation in S. Hence S is closed under the operation.

As the elements of S are also elements of G and the elements of G satisfy the associative law for the binary operation, therefore the elements of S also will satisfy the associative law.

Now $a \in S$ implies $a^{-1} \in S$.

Thus every element $a \in S$ has its inverse a^{-1} in S.

From condition (i), we have

$a \in S, a^{-1} \in S$ imply $a * a^{-1} \in S$.

But $a * a^{-1} = e$, e being the identity element of G.

Hence the identity $e \in S$.

Thus all the conditions being satisfied, S is a sub-group of G.

Theorem 4. *The necessary and sufficient condition for a non-empty sub-set S of a group $(G, *)$ to be a sub-group is*

$$a \in S, b \in S \Rightarrow a * b^{-1} \in S,$$

where b^{-1} is the inverse of b in G.

Let S be a sub-group and $a \in S$, $b \in S$. Since S is a sub-group and $b \in S$, b^{-1} must exist and will belong to S.

Now $a \in S, b^{-1} \in S \Rightarrow a * b^{-1} \in S$, by closure property.

Thus the condition is *necessary*.

To prove that this condition is also *sufficient*, we assume that

$$a \in S, b \in S \Rightarrow a * b^{-1} \in S.$$

We are to show that S is a sub-group of G.

By the given condition, we have

$$a \in S, a \in S \Rightarrow a * a^{-1} \in S, \text{ putting } b = a$$
$$\Rightarrow e \in S,$$

where e is the identity element.

Again we have $e \in S, a \in S \Rightarrow ea^{-1} \in S$

$$\Rightarrow a^{-1} \in S,$$

where a^{-1} is the inverse of a.

Now, if $b \in S$, then $b^{-1} \in S$.

Also $a \in S, b^{-1} \in S \Rightarrow a * \left(b^{-1}\right)^{-1} \in S$

$$\Rightarrow a * b \in S \text{ (closure property).}$$

Now $S \subset G$ and the associative law holds good for G, as G is a group.

Hence it is true for the elements of S. Thus all postulates for a group are satisfied for S. Hence S is a sub-group of G.

Note. In additive composition, the above condition becomes

$$a \in S, b \in S \text{ implies } a - b \in S.$$

Theorem 5. *The intersection of any two sub-groups of a group $(G, *)$ is again a sub-group of $(G, *)$.*

Let S_1 and S_2 form any two sub-groups of $(G, *)$.

We have $S_1 \cap S_2 \neq \phi$, since $e \in S_1$ and $e \in S_2$.

Let $a \in S_1 \cap S_2$ and $b \in S_1 \cap S_2$.

Now $a \in S_1 \cap S_2 \Rightarrow a \in S_1$ and $a \in S_2$,

$b \in S_1 \cap S_2 \Rightarrow b \in S_1$ and $b \in S_2$.

Since S_1 and S_2 form sub-groups under the group $(G, *)$, we have

$$a \in S_1, b \in S_1 \Rightarrow ab^{-1} \in S_1,$$
$$a \in S_2, b \in S_2 \Rightarrow ab^{-1} \in S_2.$$

Finally, $ab^{-1} \in S_1,\ ab^{-1} \in S_2 \Rightarrow ab^{-1} \in S_1 \cap S_2$.

Thus we see

$$a \in S_1 \cap S_2,\ b \in S_1 \cap S_2 \Rightarrow ab^{-1} \in S_1 \cap S_2.$$

Therefore $S_1 \cap S_2$ forms a sub-group under $(G, *)$.

Theorem 6. *The union of two sub-groups is a sub-group if and only if one is contained in the other.*

Let S_1 and S_2 form sub-groups of a group $(G, *)$.

Let $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$. Then $S_1 \cup S_2 = S_2$ or S_1.

But S_1 and S_2 form sub-groups, so that $S_1 \cup S_2$ is also a sub-group.

Next let $S_1 \cup S_2$ form a sub-group of a group $(G, *)$.

If possible, let $S_1 \not\subset S_2$ and $S_2 \not\subset S_1$.

Now $S_1 \not\subset S_2 \Rightarrow \exists\ a \in S_1$ and $a \not\subset S_2$ ... (1)

and $S_2 \not\subset S_1 \Rightarrow \exists\ b \in S_2$ and $b \not\subset S_1$. ... (2)

Here the symbol $\exists$ denotes 'there exists some'.

Therefore $a \in S_1 \cup S_2$ and $b \in S_1 \cup S_2$.

Now $S_1 \cup S_2$ has been assumed to form a sub-group.

Therefore $ab = c \in S_1 \cup S_2$.

But $ab = c \in S_1 \cup S_2 \Rightarrow ab = c \in S_1$ or S_2.

Let $ab = c \in S_1$.

Then $b = a^{-1}c \in S_1$, since S_1 forms a sub-group and $a^{-1} \in H$.

But this contradicts (2).

Hence either $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.

Note. Consider the group (Z, +).

2Z is a non-empty sub-set of Z.

Now $a \in 2Z,\ b \in 2Z \Rightarrow a + b \in 2Z$.

Also $a \in 2Z \Rightarrow -a \in 2Z$.

Therefore 2Z forms a sub-group of (Z, +).

Similarly, 3Z and in general, mZ, $m \geq 0$, forms a sub-group of (Z, +). But their union $2Z \cup 3Z$ is not a sub-group of (Z, +), since

$$2 + 3 = 5 \notin 2Z \cup 3Z.$$

3.19. Cyclic group.

A *cyclic group* is a group, in which every element can be generated by a single element of the group. The single element is called the *generator* of the cyclic group.

If a group G contains an element a such that every element $x \in G$ is of the form a^n (in multiplicative notation) or $x = na$ (in additive notation), where n is some integer, then a is called the generator of G. There may be more than one generator of a cyclic group.

If a be the generator of the cyclic group, then the group is denoted by the symbol $G = \langle a \rangle$ or $\{a\}$.

We have seen earlier that the set $S = \{1, 2, 3, 4\}$ forms a group for the operation multiplication (mod 5). Now, for this operation, we notice that

$$2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1 \pmod 5.$$

Thus the elements 1, 2, 3, 4 of the set S which forms a group can be expressed as powers of 2. We say that 2 generates the elements of a group which is called a cyclic group and its generator is 2.

The additive group Z of all integers is a cyclic group generated by 1, since $1 \in Z$ and for every integer n, we have $n = n1$.

If the binary operation be an ordinary multiplication, then each element of the cyclic group is some positive or negative power of the generator. For example, if x be the generator, then the elements of the cyclic group $\langle x \rangle$ will be of the form

$$\ldots\ldots, x^{-3}, x^{-2}, x^{-1}, x^0 = e,\quad x^1, x^2, x^3, \ldots\ldots$$

If the operation be an ordinary addition, then elements of the cyclic group $\langle x \rangle$ will be of the form

$$\ldots\ldots, (-3)x, (-2)x, (-1)x, 0x = 0, 1x, 2x, 3x, \ldots\ldots$$

A cyclic group G contains precisely all the powers a^n for some suitable $a \in G$, n being an integer. If only a finite number of elements $a^n \in G$ be distinct, then the cyclic group is *finite*, otherwise it is *infinite*. An example of the former is $[\{1, -1, i, -i\}, \cdot]$, while the example of the latter is $(Z, +)$.

Theorem 1. *A cyclic group is necessarily abelian.*

Let x, y be two elements of a cyclic group, whose generator is a.

Then there exist integers p, q such that

$$a^p = x \quad \text{and} \quad a^q = y.$$

Since $xy = a^p \cdot a^q = a^{p+q} = a^q \cdot a^p = yx$,

therefore $xy = yx$, for all x, y of the cyclic group.

Hence it is abelian.

The converse of this theorem is not true ; for example, Klein 4-group and $(Q, +)$ are abelian groups but not cyclic.

Theorem 2. *The order of the cyclic group is the same as the order of its generator.*

Let the cyclic group $G = \{a\}$ and $o(a) = n$, a finite quantity, so that

$$a^n = e, \text{ the identity of } G.$$

We shall show that G is also of finite order and $o(G) = n$.

By Division Algorithm, we write any integer s as $s = nq + r$, where q and r are unique integers and $0 \le r < n$. Then we have

$$a^s = a^{nq+r} = \left(a^n\right)^q a^r = e^q a^r = a^r, \text{ since } a^n = e.$$

Also, by definition, $G = \{a\} = \{a^k : k \text{ is an integer}\}$.

Hence there are exactly n elements in G of the form a^r, where $0 \le r < n$.

Thus the order of G is the same as the order of a and

$$G = \left\{a^0 = e, a, a^2, \ldots\ldots, a^{n-1}\right\}.$$

Again, let the order of G be infinite, so that there exists no positive integer n such that $a^n = e$. We shall now show that $a, a^2, a^3, \ldots\ldots$ are all distinct. For, if $a^r = a^s$, where r and s are positive integers and $r > s$, then multiplying by a^{-s}, we have

$$a^r a^{-s} = a^s \cdot a^{-s}$$

or, $$a^{r-s} = e, \text{ with } r - s > 0.$$

This contradicts our assumption that $o(a) = \infty$.

Hence G consists of an infinite number of elements, that is, the order of G is infinite.

Theorem 3. *If G be a finite cyclic group of order n generated by a, then a^m is a generator of G, iff m be prime to n.*

First we assume that m is prime to n and $H = \{a^m\}$. Since each integral power of a^m is also an integral power of a and $G = \{a\}$, we have

$$H \subseteq G. \quad \ldots (1)$$

As m is prime to n, there exist two integers x and y, such that

$$xm + yn = 1.$$

Therefore $a^{xm+yn} = a$, that is, $a^{xm} \cdot a^{yn} = a$.

Hence $(a^m)^x = a$, since $a^{yn} = (a^n)^y = e^y = e$.

This shows that $G \subseteq H$. ... (2)

From (1) and (2), we have $G = H$ and $G = \{a^m\}$.

Next we suppose that $G = \{a^m\}$.

We suppose, if possible, m is not prime to n. Then m and n will have a greatest common divisor d, where $d \neq 1$, which implies $d > 1$.

This gives that $\frac{m}{d}$ and $\frac{n}{d}$ must be positive integers.

Now $(a^m)^{\frac{n}{d}} = (a^n)^{\frac{m}{d}} = e^{\frac{m}{d}} = e$.

Evidently, $\frac{n}{d}$ is a positive integer less than n. Hence $o(a^m) < n$.

Consequently, a^m cannot be a generator of G, because the order of a^m is not equal to that of G, which contradicts our assumption. Hence m must be prime to n.

Cor. The number of generators of a cyclic group of order n is equal to the number of integers less than n and prime to n. For example, a is a generator of the cyclic group $G = \{a, a^2, a^3, ..., a^8 = e\}$. Here a, a^3, a^5, a^7 are the generators, since 3, 5, 7 are integers less than 8 and prime to 8.

Theorem 4. *If G be an infinite cyclic group, then G has exactly two generators.*

Let $G = \{a\}$ be an infinite cyclic group, so that the elements of G are some integral powers of a. We shall show that no two distinct integral powers of a can be equal. If possible, let $a^r = a^s, r > s$.

This implies $a^r \cdot a^{-s} = a^s \cdot a^{-s}$,

that is, $a^{r-s} = a^0 = e$.

This shows that $o(a) \leq r - s$, which implies that $o(a)$ is finite and hence a cannot be a generator of the infinite cyclic group G. Therefore $a^r \neq a^s$ unless $r = s$. Hence we can write

$$G = \{....., a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, ...\}.$$

If now a^m be any element of G, then we can write

$$a^m = (a^{-1})^{-m}$$

showing that every element of G can be expressed as an integral power of a^{-1}.

Hence a^{-1} is also a generator of G. a and a^{-1} being two distinct elements, G has two distinct generators a and a^{-1}.

Now we show that a^m cannot be a generator of G, if $m \neq 1$ or (-1). If a^m is to be a generator of G, then there must exist an integer k such that $\left(a^m\right)^k = a$, that is, $a^{mk} = a$.

Now $m \neq 1$ or (-1) implies $mk \neq 1$.

Thus two distinct integral powers of a, namely, a^{mk} and a are equal which cannot be as has been proved before. Hence a^{mk} cannot be a generator of G, if $m \neq 1$ or (-1).

Thus G has exactly two generators a and a^{-1}.

Note. The only two integers of the additive group of integers are 1 and (-1).

Theorem 5. *Every sub-group of a cyclic group is cyclic.*

Let H be a sub-group of the cyclic group $G = < a >$ whose generator is a. Now, if s be an integer, then every element of G, hence also of H, will be of the form a^s.

Let m be the smallest positive integer, such that $a^m \in H$. We shall show that $H = < a^m >$ for which we shall show that if $a^s \in H$, then $s = mh$; in that case $a^s = \left(a^m\right)^h$.

If s be not divisible by m, then there exist integers q and r such that

$$s = mq + r, \quad 0 \leq r < m.$$

Then $$a^s = a^{mq+r} = a^{mq}.a^r.$$

Therefore $$a^r = a^s \cdot \left(a^{mq}\right)^{-1}.$$

Now, since $a^m \in H$, then $a^{mq} \in H$ and hence its inverse $\left(a^{mq}\right)^{-1} \in H$.

But we have supposed that $a^s \in H$; hence, from above, $a^r \in H$. This is contrary to the choice of m, since m is the least positive integer such that $a^m \in H$, by assumption.

Hence $r = 0$ and so $s = mq$.

But then $a^s = \left(a^m\right)^q$. Thus every element a^s of H is of the form $\left(a^m\right)^q$.

Hence we have

$$H = < a^m >.$$

3.20. Cosets.

Let H be a sub-group of a group G under certain composition and let $a \in G$. Then the set $\{ah : h \in H\}$ is called the *left coset* generated by a and H and is denoted by aH.

Similarly, the set $\{ha : h \in H\}$ is the *right coset* and is denoted by Ha.

It is evident that both aH and Ha are sub-sets of G. If the group operation be addition, then the left coset of H in G is the set $\{a+h : h \in H\}$ and is denoted by $(a + H)$. For a right coset, the set is $\{h+a : h \in H\}$ which is denoted by $(H + a)$.

Since $eH = H = He$, e being the identity of the group, we see that H is itself a left as well as a right coset.

In general, $aH \neq Ha$. But in the case of abelian group, each left coset coincides with the corresponding right coset.

Consider the additive group of integers, given by

$$I = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}.$$

Let H be the sub-group of I consisting of the even integers and

$$H = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}.$$

Since I is abelian, the left cosets will coincide with the corresponding right cosets. The identity of I is 0.

The right cosets of H in I are the following :

$$H = H + 0 = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}, 0 \in I,$$

$$H + 1 = \{\ldots\ldots, -5, -3, -1, 1, 3, 5, 7, \ldots\ldots\}, 1 \in I.$$

We see that right cosets H and $(H + 1)$ are disjoint.

Again $H + 2 = \{\ldots\ldots, -4, -2, 0, 2, 4, 6, \ldots\ldots\}, 2 \in I$.

We observe that $H + 2 = H$.

Also $H + 3 = \{\ldots\ldots, -3, -1, 1, 3, 5, 7, \ldots\ldots\}, 3 \in I$.

Here too we observe that $H + 3 = H + 1$.

By constructing other right cosets, we can verify that $H + 4 = H$, $H + 5 = H + 1$, and so on. Thus there are only two distinct cosets, H and $(H + 1)$, so that $I = H \cup (H + 1)$.

In a similar way, we can verify that

$$I = H \cup (H+1) \cup (H+2) \cup \ldots\ldots \cup (H+m-1),$$

where H is the sub-group of I consisting of all the multiplies of a given integer m.

Theorem 1. *If H be a sub-group of a group G and $h \in H$, then*

$$hH = Hh = H.$$

Let h' be an arbitrary element of H, so that from definition of left coset, we have $hh' \in hH$.

Since H is a sub-group, we have

$$h \in H, h' \in H \Rightarrow hh' \in H.$$

Therefore every element of hH is also an element of H and we have

$$hH \subset H. \quad \ldots (1)$$

Again $h' = (hh^{-1})h' = h(h^{-1}h') \in hH$,

since $h^{-1} \in H, h' \in H \Rightarrow h^{-1}h' \in H$.

We can conclude then that every element of H is also an element of hH.

Hence $H \subset hH$. $\ldots (2)$

From (1) and (2), it follows that $hH = H$.

Similarly, it can be shown that $Hh = H$.

Theorem 2. *Any two left (or right) cosets of a sub-group are either disjoint or identical.*

Let H be a sub-group of a group G and let aH and bH be two of its left cosets. Assume that $aH \cap bH \neq \phi$ and let c be the common element of the two cosets.

Then we may write $c = ah$ and $c = bh'$, for $h, h' \in H$.

Therefore $ah = bh'$, giving $a = bh'h^{-1}$.

Since H is a sub-group, we have $h'h^{-1} \in H$.

Let $h'h^{-1} = h''$, so that $a = bh''$.

Hence $aH = (bh'')H = b(h''H) = bH$, since $h''H = H$.

Hence the two left cosets aH and bH are identical, if $aH \cap bH \neq \phi$.

Thus either $aH \cap bH \neq \phi$ or $aH = bH$.

The theorem can be proved for right cosets similarly.

3.21. Coset decomposition.

We have seen that any two left (or right) cosets of a sub-group H of G are either identical or disjoint. As a consequence, the set of all left (or right) cosets of H results decomposition of G into mutually disjoint classes. In fact, the partition of a group G into mutually disjoint classes known as cosets is accomplished by defining an equivalence relation known as congruence relation.

Let H be a sub-group of a group G and let $a, b \in G$. We say "a is congruent to b modulo H", if $ab^{-1} \in H$ and write

$$a \equiv b \mod H.$$

It can be shown that this congruence relation is an equivalence relation in the corresponding group.

The number of left (or right) cosets of the sub-group H in G is called the *index* of H in G and is denoted by $(G : H)$.

Consider the sub-group H in the group G. H itself is a right coset. If we find an element $a \in G$ and $a \notin H$, then Ha will be another distinct right coset. If again we can find an element $b \in G$ and $b \notin H$ and also $b \notin Ha$, then Hb will be another distinct right coset. In this way, we can get all the distinct right cosets of H in G. Thus

$$G = H \cup Ha \cup Hb \cup .....$$

Thus we have obtained a *right coset decomposition* of G.

Similarly, we can get a *left coset decomposition* of G.

3.22. Lagrange's theorem.

The order of each sub-group of a finite group G is a divisor of the order of the group G.

Let G be a finite group of order n and H be any sub-group of G whose order is m. Let us consider the left coset decomposition of G relative to H.

Let $H = \{h_1, h_2, ..., h_m\}$.

Then the m members of $aH (a \in G)$ are

$$ah_1, ah_2, ..., ah_m.$$

These members are all distinct, since

$$ah_i = ah_j \Rightarrow h_i = h_j,$$

by the cancellation law in G.

Now, G being a finite group, the number of distinct left cosets is also finite. Let this number be k, so that the total number of elements of the m cosets is km and this is the total number of elements of G.

Therefore $n = mk$.

This proves that the order of H, that is m, is a divisor of n which is the order of the group G.

Note. The converse of Lagrange's theorem is not true.

For instance, a group of order 12 exists which has no sub-group of order 6.

Cor. 1. The index k of a sub-group H of a finite group G is a divisor of the order of G.

Cor. 2. The order of every element of a finite group is a divisor of the order of the group.

Cor. 3. If G be a finite group of order n and $a \in G$, then

$$a^n = e.$$

Let $o(a) = m$, which implies $a^m = e$.

Now the sub-set H of G consisting of all the integral powers of a is a sub-group of G and the order of H is m.

Then, by the above theorem, m is a divisor of n.

Let $n = mk$; then

$$a^n = a^{mk} = \left(a^m\right)^k = e^k = e, \text{ since } o(a) = m.$$

Cor. 4. *Fermat's little theorem*: If p be a prime and be not a divisor of an integer a, then $a^{p-1} \equiv 1 (\text{mod}\, p)$.

By division algorithm, we have $a \equiv pq + r$, where q and r are integers and $0 < r < p$, (since $r = 0$ gives trivial result).

Thus $a \equiv r (\text{mod}\, p)$.

Hence, by Cor. 3 above, we get the result.

3.23. Normal sub-group.

Let G be a multiplicative abelian group and H be a sub-group of G. If x be any element of G, then Hx is the right coset of H in G and xH is a left coset of H in G. Now, since G is abelian, $Hx = xH \ \forall \ x \in G$. But it may so happen that G is not abelian yet it may have a sub-group G, such that for any $x \in G, Hx = xH$. This gives rise to a class of sub-groups of G which comes under the class of normal sub-groups.

A sub-group H of a group G is said to be a *normal sub-group of* G, if, for every $x \in G$ and for every $h \in H$,

$$x h x^{-1} \in H.$$

The definition is equivalent to saying that H is a normal sub-group of the group G, if and only if $x H x^{-1} \subset H \ \forall \ x \in G$.

If $x H x^{-1} = H \ \forall \ x \in G$, then truly $x H x^{-1} \subset H$ and so, by definition, H is a normal sub-group of G.

In this case, we have

$$\left(x H x^{-1}\right) x = Hx \qquad \text{or} \qquad xH = Hx \ \forall \ x \in G.$$

Hence each left coset xH is the right coset Hx.

Again, let G be an abelian group and H be a sub-group of G. G being abelian, we have $xH = Hx \ \forall \ x \in G$. Thus H is a normal sub-group in G.

Further, since every cyclic group is abelian, we observe that every sub-group of a cyclic group is normal.

We have seen earlier that $3Z$ is a sub-group of the group $(Z, +)$. Since $(Z, +)$ is abelian, $3Z$ is a normal sub-group.

Theorem. *The intersection of two normal sub-groups of a group G is a normal sub-group of G.*

Let H and K be two normal sub-groups of G.

Since the intersection of two sub-groups of G is a sub-group of G, therefore $H \cap K$ is a sub-group of G.

Let $x \in G$. Then, from $H \cap K \subseteq H$, we have

$x (H \cap K) x^{-1} \subseteq H$, since H is a normal sub-group of G.

Similarly, $x (H \cap K) x^{-1} \subseteq K$.

Hence $x (H \cap K) x^{-1} \subseteq H \cap K$.

Therefore $H \cap K$ is normal in G.

If $a \in G$, then the *normalizer* of a in G is the set of all elements in G that commute with a and is denoted by $N(a)$.

Thus $N(a) = \{x \in G : x a = a x\}$.

The normalizer of H in G is written as

$$N_G(H) = \left\{x \in G : x H x^{-1} = H\right\}.$$

It is a sub-group of G.

If H be a normal sub-group of G, then $N_G(H) = H$.

Let H be a normal sub-group of a group G. Then the set of left cosets (or the set of right cosets) of H in G is also a group called the *factor group* or the *quotient group* of G by H and is denoted by G/H.

If G be a finite group, then $o(G/H) = \frac{o(G)}{o(H)}$.

3.24. Cauchy's theorem for finite abelian groups.

If G be a finite abelian group and p be a prime number that divides the order of G, then G has an element of order p.

This is proved by using the second principle of mathematical induction.

The theorem is true when $o(G) = 2$.

We assume that it is true for all abelian groups with fewer elements than G and use this assumption to show that it is true for G as well. Certainly, G has elements of prime order, since if $o(a) = m$ and $m = qn$, where q is prime, then $o(a^n) = q$.

Let a be an element of G of some prime order $q\ (\neq p)$.

Now every sub-group of an abelian group is normal. So we may construct the factor group $\overline{G} = \frac{G}{<a>}$, which is abelian.

Since $o(\overline{G}) = \frac{o(G)}{q}$, therefore p divides $o(\overline{G})$ and hence, by induction, $\overline{G}$ has an element, say, $b<a>$, of order p.

Then $(b<a>)^p = b^p <a> = <a>$ and therefore $b^p \in <a>$.

If $b^p = e$, then the theorem is proved.

If $b^p \neq e$, then b^p has order q and b^q has order p.

3.25. Homomorphism and isomorphism of groups.

Let $(G, *)$ and $(G', *')$ be two groups and $\phi : G \to G'$ be a mapping from G to G'. If $\phi(a * b) = \phi(a) *' \phi(b)$ for all $a, b \in G$, then the mapping ϕ is said to be a *homomorphism* of the group G into the group G'.

Here the elements of G are used in the operation on the left hand side of the relation whereas those of G' are used in the operation on the right hand side of the relation.

As an example of homomorphism, we consider an additive group G of integers and a cyclic group G' generated by an element a. Then, for integers m and $n \in G$, we have $\phi : G \to G'$ in which $\phi(m) = a^m$. Then $\phi(m+n) = a^{m+n} = a^m . a^n = \phi(m)\,\phi(n)$. Here ϕ is a homomorphism of the group G into the group G'.

The *kernel* of a homomorphism ϕ from a group G to a group G' with identity e' is the set $\{a \in G : \phi(a) = e'\}$. It is written as $\ker\phi$. Thus $\ker\phi$ is the set of the elements of G which are mapped to the identity element of G'.

A group homomorphism of $\phi : G \to G'$ is a one-to-one mapping, if and only if $\ker \phi = \{e\}$.

If R^* be the group of non-zero real numbers under multiplication, then the mapping ϕ, defined by $\phi(x) = |x|$ from R^* to R^*, is a homomorphism with $\ker \phi = \{1, -1\}$.

Let $(G, *)$ and $(G', *')$ be two groups and $\phi : G \to G'$ be a homomorphism. Then the sub-set $\{\phi(a) : a \in G\}$ of G' is called the *image* of ϕ and is denoted by $I_m\,\phi$ or $\phi(G)$. Thus $I_m\,\phi = \{\phi(a) : a \in G\}$ and is a sub-group of G'.

Some properties of homomorphisms

Let ϕ be a homomorphism of a group G into a group G'.

(i) *If e be the identity element of G, then $\phi(e)$ is the identity element of G'.*

Here $e * e = e$ in G.

Since ϕ is a homomorphism, we have, therefore

$$\phi(e) *' \phi(e) = \phi(e) \text{ in } G'.$$

Hence $\phi(e) *' \phi(e) = \phi(e) *' e'$, if e' be the identity element of G'.

So, by left cancellation law, we get $\phi(e) = e'$.

(ii) *If $a \in G$, then $\phi(a^{-1}) = \{\phi(a)\}^{-1}$.*

Let e be the identity element of G and e' be that of G'.

Then $\phi(e) = \phi(a * a^{-1}) = \phi(a) *' \phi(a^{-1})$.

Also $\phi(e) = \phi(a^{-1} * a) = \phi(a^{-1}) *' \phi(a)$.

Therefore

$\phi(a) *' \phi(a^{-1}) = \phi(a^{-1}) *' \phi(a) = e'$ in G', by property (i).

Hence, by definition, $\phi(a^{-1})$ is the inverse of $\phi(a)$ in G',

that is, $\phi(a^{-1}) = \{\phi(a)\}^{-1}$.

(iii) If $a \in G$ and n be an integer, then $\phi(a^n) = \{\phi(a)\}^n$.

If n be a positive integer, then this can be proved by the method of induction.

If n be a negative integer, let $n = -m$, where m is a positive integer.

Then $\phi(a^n) = \phi(a^{-m}) = \phi\{(a^{-1})^m\} = \{\phi(a^{-1})\}^m$, since m is a positive integer

$$= \left[\{\phi(a)\}^{-1}\right]^m, \text{ by property } (ii)$$

$$= \{\phi(a)\}^{-m} = \{\phi(a)\}^n.$$

(iv) If $a \in G$ and $o(a)$ be finite, then order of $\phi(a)$ is a divisor of $o(a)$.

Let $o(a) = n$, so that $a^n = e$, if e be the identity element of G.

So $\phi(a^n) = \phi(e) = e'$, if e' be the identity element of G'.

Therefore $\{\phi(a)\}^n = e'$.

Hence $\phi(a)$ is of finite order and order of $\phi(a)$ is a divisor of n, that is, divisor of $o(a)$.

(v) $\ker\phi$ is a sub-group of G.

Let e be the identity element of G and e' be that of G'.

Since $e \in \ker\phi$, so $\ker\phi$ is a non-empty sub-set of G.

Let $a, b \in \ker\phi$.

Then $\phi(a * b^{-1}) = \phi(a) *' \{\phi(b)\}^{-1} = e' *' (e')^{-1} = e'$.

Hence $a * b^{-1} \in \ker\phi$, showing that $\ker\phi$ is a sub-group of G.

It can also be shown that $\ker\phi$ is normal in G.

Let ϕ be a homomorphism of a group G into a group G'. If the mapping ϕ be injective, then the homomorphism is said to be a *monomorphism*. When the mapping ϕ is surjective, then the homomorphism is said to be an *epimorphism*. If the mapping ϕ be bijective, then the homomorphism is said to be an *isomorphism*.

Thus a homomorphism is said to be an isomorphism, if it be both monomorphism and epimorphism.

An isomorphism from a group G onto itself is called an *automorphism* of G.

Two groups G and G' are said to be *isomorphic*, if there exists an isomorphism ϕ from G to G'.

The additive group of integers

$$G = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$$

is isomorphic to the additive group

$$G' = \{\ldots\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\ldots\}.$$

Here $\phi: G \to G'$ is defined by $\phi(a) = 2a \; \forall \; a \in G$.

If a_1 and $a_2 \in G$, then $a_1 \neq a_2$ implies $2a_1 \neq 2a_2$ and hence

$$\phi(a_1) \neq \phi(a_2).$$

Therefore ϕ is one - one.

Again, if $x \in G'$, then $\frac{1}{2}x \in G$.

So $x \in G'$ shows that $\frac{1}{2}x \in G$ such that ϕ - image of $\frac{1}{2}x$ is x.

Thus each element of G' is the ϕ - image of some element of G and hence ϕ is onto.

For any two elements a_1 and $a_2 \in G$, we have

$$\phi(a_1 + a_2) = 2(a_1 + a_2) = 2a_1 + 2a_2 = \phi(a_1) + \phi(a_2).$$

Therefore ϕ preserves the compositions in G and G'.

Hence G is isomorphic to G'.

Some properties of isomorphisms

Let $(G, *)$ and $(G', *')$ be two groups and $\phi: G \to G'$ be an isomorphism.

(*i*) G' *is commutative if and only if* G *be commutative.*

First we suppose that G' is commutative and $a, b \in G$.

Then $\phi(a * b) = \phi(a) *' \phi(b) = \phi(b) *' \phi(a)$, since G' is commutative

$= \phi(b * a)$.

This implies $a * b = b * a$, since ϕ is one-to-one.

This holds for all $a, b \in G$. Hence G is commutative.

Next we suppose that G is commutative and $a', b' \in G'$.

Since ϕ is an isomorphism, there exist unique elements a, b in G such that $\phi(a) = a', \phi(b) = b'$.

Now $a' *' b' = \phi(a) *' \phi(b) = \phi(a * b)$, since ϕ is a homomorphism

$= \phi(b * a)$, since G is commutative

$= \phi(b) *' \phi(a) = b' *' a'$.

This holds for all $a', b' \in G'$. Hence G' is commutative.

(*ii*) G' *is cyclic if and only if* G *be cyclic.*

Let G' be cyclic and $G' = \langle a' \rangle$.

Since ϕ is an isomorphism, there exists a unique element a in G such that $\phi(a) = a'$.

If $b \in G$, then $\phi(b) \in G'$ and $\phi(b) = (a')^m$ for some integer m.

Hence $\phi(b) = \{\phi(a)\}^m = \phi(a^m)$.

Therefore $b = a^m$, since ϕ is one-to-one.

So every element of G is of the form a^n, where n is an integer.

Therefore G is cyclic and $G = \langle a \rangle$.

Conversely, let G be cyclic and $G = \langle a \rangle$. Let $b' \in G'$.

Since ϕ is an isomorphism, there exists a unique element b in G such that $\phi(b) = b'$.

Since $b \in G$, we have $b = a^m$ for some integer m.

Thus $b' = \phi(b) = \phi(a^m) = \{\phi(a)\}^m$.

So every element of G' is of the form $\{\phi(a)\}^n$, where n is an integer.

Hence G' is cyclic and $G' = \langle \phi(a) \rangle$.

It is to be noted that if a be a generator of G, then $\phi(a)$ is a generator of G'.

(iii) For all $a \in G$, the order of a is equal to the order of $\phi(a)$, that is,

$$o(a) = o\{\phi(a)\}.$$

Let e be the identity element of G and e' be that of G'.

Let $o(a) = n$. Then $a^n = e$, n being the least positive integer.

Since ϕ is a homomorphism, therefore

$$\{\phi(a)\}^n = \phi(a^n) = \phi(e) = e'.$$

Hence $o\{\phi(a)\}$ is a divisor of n.

We are to show that $o\{\phi(a)\} = n$.

If possible, let $o\{\phi(a)\} = m$, where $m < n$.

Then $e' = \{\phi(a)\}^m = \phi(a^m)$.

Since ϕ is an isomorphism, ϕ is one-to-one and therefore $a^m = e$, which contradicts that $o(a) = n$. Hence $o\{\phi(a)\} = n$.

(iv) The sets G and G' have the same cardinal number.

This follows from the fact that $\phi : G \to G'$ is a bijection, since ϕ is an isomorphism.

(v) The inverse mapping $\phi^{-1} : G' \to G$ is also an isomorphism.

Since ϕ is a bijective mapping from G to G', ϕ^{-1} exists and $\phi^{-1} : G' \to G$ is also bijective.

Let $a', b' \in G'$ and $\phi^{-1}(a') = a$, $\phi^{-1}(b') = b$.

Then $\phi(a) = a'$, $\phi(b) = b'$.

Now $\phi^{-1}(a' *' b') = \phi^{-1}\{\phi(a) *' \phi(b)\} = \phi^{-1}\{\phi(a * b)\}$,

since ϕ is a homomorphism

$= a * b = \phi^{-1}(a') * \phi^{-1}(b')$,

which shows that ϕ^{-1} is a homomorphism.

Since ϕ^{-1} is a bijection, therefore ϕ^{-1} is an isomorphism.

3.26. Cayley's theorem.

Every finite group is isomorphic to a sub-group of a permutation group.

In other words, a group G of order n is isomorphic to a sub-group of the symmetric group S_n.

Let $G = \{g_1, g_2, g_3, \ldots\ldots, g_n\}$ and e be the identity element and g be an arbitrary element of G.

Then the elements $gg_1, gg_2, gg_3, \ldots\ldots, gg_n$ (no two of which are equal) all belong to G.

Therefore $\begin{pmatrix} g_1 & g_2 & g_3 & \ldots\ldots & g_n \\ gg_1 & gg_2 & gg_3 & \ldots\ldots & gg_n \end{pmatrix}$ is a permutation on the set $\{g_1, g_2, g_3, \ldots\ldots, g_n\}$.

This permutation is denoted by θ_g.

Let S_n be the set of all permutations on the set

$$\{g_1, g_2, g_3, \ldots\ldots, g_n\}.$$

Let us define a mapping $\phi : G \to S_n$ by $\phi(g_r) = \theta_{g_r}$.

So $\phi(g_r) = \begin{pmatrix} g_1 & g_2 & g_3 & \ldots\ldots & g_n \\ g_r g_1 & g_r g_2 & g_r g_3 & \ldots\ldots & g_r g_n \end{pmatrix}$ for $r = 1, 2, 3, \ldots\ldots, n$.

Now let $g_r, g_s \in G$. Then $g_r\, g_s \in G$ and

$$\phi(g_r g_s) = \begin{pmatrix} g_1 & g_2 & g_3 & \ldots\ldots & g_n \\ g_r g_s g_1 & g_r g_s g_2 & g_r g_s g_3 & \ldots\ldots & g_r g_s g_n \end{pmatrix}$$

$$= \begin{pmatrix} g_1 & g_2 & \ldots\ldots & g_n \\ g_r g_1 & g_r g_2 & \ldots\ldots & g_r g_n \end{pmatrix} * \begin{pmatrix} g_1 & g_2 & \ldots\ldots & g_n \\ g_s g_1 & g_s g_2 & \ldots\ldots & g_s g_n \end{pmatrix}$$

$$= \phi(g_r) * \phi(g_s),$$

which shows that ϕ is a homomorphism.

For $a \in G$, $a \in \ker\phi \Leftrightarrow \phi(a) = \begin{pmatrix} g_1 & g_2 & \ldots\ldots & g_n \\ g_1 & g_2 & \ldots\ldots & g_n \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} g_1 & g_2 & \ldots\ldots & g_n \\ ag_1 & ag_2 & \ldots\ldots & ag_n \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & \ldots\ldots & g_n \\ g_1 & g_2 & \ldots\ldots & g_n \end{pmatrix}$$

$\Leftrightarrow ag_i = g_i$ for $i = 1, 2, 3, \ldots\ldots, n$

$\Leftrightarrow a = e$.

Hence $\ker\phi = e$ and so ϕ is a monomorphism.

Therefore $\phi(G)$ is a sub-group of S_n and thus G is isomorphic to a sub-group of S_n.

Note 1. The sub-group $\phi(G)$ is $\{\theta_{g_1}, \theta_{g_2}, \theta_{g_3}, \ldots\ldots, \theta_{g_n}\}$.

Note 2. It is difficult to use this theorem, since the order of S_n is usually very large in comparison to n.

3.27. Isomorphism theorems for groups.

First theorem. *If G and G' be two groups and $\phi : G \to G'$ be an epimorphism with kernel K, then the factor group G/K and the group G' are isomorphic.*

The kernel K of the epimorphism ϕ is a normal sub-group of G.

We define a mapping $\Psi : G/K \to G'$ by letting $\Psi(Ka) = \phi(a)$ for all $Ka \in G/K$ and $a \in G$.

Ψ is well-defined, if $Ka = Kb$ (for $a, b \in G$) implies that $\phi(a) = \phi(b)$, that is, $\Psi(Ka) = \Psi(Kb)$.

Now $Ka = Kb \Rightarrow b = ka$ for $k \in K$ and then

$$\phi(b) = \phi(ka) = \phi(k)\,\phi(a) = e'\phi(a),$$

where e' is the identity element of G'

$$= \phi(a)$$

or, $\Psi(Ka) = \Psi(Kb)$, showing that Ψ is well-defined.

For $a, b \in G$, we have

$$\Psi(KaKb) = \Psi(Kab) = \phi(ab) = \phi(a)\,\phi(b) = \Psi(Ka)\Psi(Kb).$$

So Ψ is a homomorphism.

Again, the mapping Ψ is injective, since, for $a, b \in G$,

$\Psi(Ka) = \Psi(Kb) \Rightarrow \phi(a) = \phi(b)$ and so

$\phi(ab^{-1}) = \phi(a)\{\phi(b)\}^{-1} = e'$, where e' is the identity element of G', giving $ab^{-1} \in K$ and $Ka = Kb$.

Moreover the mapping Ψ is surjective, since each element of G' is of the form $\phi(a)$ for all $a \in G$ and then $\Psi(Ka) = \phi(a)$.

Thus Ψ is an isomorphism, that is, G/K and G' are isomorphic.

Note. This theorem is also known as *fundamental theorem of group homomorphism.*

Second theorem. *If G be a group, H be a sub-group of G and N be a normal sub-group of G, then the factor groups NH/N and $H/(N \cap H)$ are isomorphic.*

Since N is a normal sub-group of G, therefore NH is a sub-group of H and $N \cap H$ is a normal sub-group of H.

We define a mapping $f : H \to NH/N$ with kernel K, that is,

$$\ker f = K .$$

We also define $f(h)$, where $h \in H$, to be the coset NH of N in the sub-group $NH = \{ nh \mid n \in N, h \in H \}$.

Now f is a homomorphism, since, for $h_1, h_2 \in H$,

$$f(h_1 h_2) = Nh_1h_2 = Nh_1Nh_2 = f(h_1) f(h_2) .$$

Again f is surjective. So f is an epimorphism.

Therefore, by the first theorem, H/K is isomorphic to NH/N.

Furthermore, if $h \in H \cap N$, then $h \in N$ and so $Nh = N$ and thus $h \in K$.

Also, if $h \in K$, then $Nk = N$ and so $k \in N$.

Thus $k \in N \cap H$. Hence $K = N \cap H$ and the theorem is proved.

Third theorem. If M *and* N, $(N \leq M)$, *be normal sub-groups of a group* G, *then* $(G/N)/(M/N)$ *is isomorphic to* G/M.

This theorem can be proved by using the first and second theorems.

3.28. Illustrative Examples.

Ex. 1. (*a*) *Show that a group* G *is abelian, if* $(ab)^2 = a^2b^2$, *for* $a, b \in G$. [C.H.1993; B.H.2004]

(*b*) *Prove that a group* G *is abelian, if* $b^{-1}a^{-1}ba = e \ \forall \ a, b \in G$.

(*a*) From the given relation $(ab)^2 = a^2b^2$, we have

$$(ab)(ab) = (aa)(bb)$$

or, $a(ba)b = a(ab)b$ (associative law)

or, $(ba)b = (ab)b$ (left cancellation law)

or, $ba = ab$ (right cancellation law).

Since a and b are arbitrary and $ba = ab$, it shows that G forms an abelian group.

(*b*) We have $b^{-1}a^{-1}ba = e \Rightarrow (b^{-1}a^{-1})(ba) = e$

$\Rightarrow (b^{-1}a^{-1})^{-1} = ba$, since $ab = e \Rightarrow a^{-1} = b$

$\Rightarrow (a^{-1})^{-1}(b^{-1})^{-1} = ba$, since $(ab)^{-1} = b^{-1}a^{-1}$

$\Rightarrow ab = ba$.

Hence G is abelian.

Ex. 2. *If, in a group G, $x^2 = e$ (identity), for all x in G [that is, if every element of G (except the identity element) be of order two], then prove that G is abelian.* [C.H. 1992, 2002]

We have $x^2 = e \Rightarrow x = x^{-1}$, for all $x \in G$.

Therefore $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Hence G is abelian.

Alternatively : Let $x, y \in G$. Then, since every element is of order two, we have $x^2 = y^2 = e$.

Further, since $xy \in G$, $(xy)^2 = e$.

Now $(xy)^2 = e$ implies $(xy)(xy) = e$, that is, $x(yx)y = e$.

This gives $x[x(yx)y]y = xey$

or, $(xx)(yx)(yy) = xy$

or, $x^2(yx)y^2 = xy$

or, $e(yx)e = xy$, since $x^2 = y^2 = e$.

Therefore $yx = xy$.

Hence G is abelian.

Ex. 3. (*a*) *If a, b be elements of a group G, then show that*

$$o(a) = o(b^{-1}ab).$$

(*b*) *Given that $axa = b$ in G, find x.*

(*a*) If a be the identity element e of the group, then

$b^{-1}ab = e$; hence $o(a) = o(b^{-1}ab)$.

If $o(a) = n$, then $a^n = e$.

Now $(b^{-1}ab)^n = (b^{-1}ab)(b^{-1}ab).....(b^{-1}ab)$ (n factors)

$= b^{-1}a^n b = b^{-1}eb = b^{-1}b$

$= e$.

If possible, let $(b^{-1}ab)^m = e$, where m is a positive integer less than n.

Then $b^{-1}a^m b = e$.

Hence $a^m = beb^{-1} = bb^{-1} = e$, which is a contradiction, since $o(a) = n$.

Therefore n is the least positive integer, such that $(b^{-1}ab)^n = e$, which gives $o(b^{-1}ab) = n$.

If $o(a)$ be infinite, then we assume, if possible,

$(b^{-1}ab)^m = e$, where m is a positive integer.

Then $b^{-1}a^m b = e$

or, $a^m = beb^{-1} = bb^{-1} = e$, which is a contradiction.

Therefore $o(b^{-1}ab)$ is infinite.

(*b*) We have $axa = b$

$$\begin{aligned}
&\Rightarrow a^{-1}(axa) &&= a^{-1}b \\
&\Rightarrow (a^{-1}a)(xa) &&= a^{-1}b \\
&\Rightarrow e(xa) &&= a^{-1}b \\
&\Rightarrow xa &&= a^{-1}b \\
&\Rightarrow (xa)a^{-1} &&= a^{-1}ba^{-1} \\
&\Rightarrow x(aa^{-1}) &&= a^{-1}ba^{-1} \\
&\Rightarrow xe &&= a^{-1}ba^{-1}.
\end{aligned}$$

This gives $x = a^{-1}ba^{-1}$.

Ex. 4. *If G be an abelian group with identity e, then prove that all elements x of G satisfying the equation $x^2 = e$ form a sub-group H of G.*

Let $H = \{x : x^2 = e\}$.

Now $x^2 = e \Rightarrow x = x^{-1}$.

Therefore, if $x \in H$, then x^{-1} also belongs to H.

Furthermore $e^2 = e$.

Hence the identity element of G also belongs to H.

Let $x, y \in H$.

Then, since G is abelian, we have

$$\begin{aligned}
xy &= yx \\
&= y^{-1}x^{-1}, \text{ as } x^{-1} = x \text{ and } y^{-1} = y \\
&= (xy)^{-1}.
\end{aligned}$$

Therefore $(xy)^2 = e$.

Hence $xy \in H$ and H is a sub-group of G.

Ex. 5. *If a be a fixed element of the group G, then show that the set*

$$N(a) = \{x \in G \mid xa = ax\} \text{ is a sub-group of } G.$$

Let $x, y \in N(a)$. Then $xa = ax$ and $ya = ay$.

Now $ya = ay \Rightarrow y^{-1}(ya)y^{-1} = y^{-1}(ay)y^{-1}$.

Therefore $ay^{-1} = y^{-1}a$. ... (1)

Hence $y^{-1} \in N(a)$.

Again $(xy^{-1})a = x(y^{-1}a) = x(ay^{-1})$, by (1)

$= (xa)y^{-1} = (ax)y^{-1} = a(xy^{-1})$.

Hence $xy^{-1} \in N(a)$, since $x, y \in N(a)$.

Therefore $N(a)$ is a sub-group of G.

Ex. 6. *If $a = (1\ 2\ 3\ 4)$, then show that the set $\{a, a^2, a^3, a^4\}$ forms a cyclic group.*

We have $a^2 = aa = \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$,

$a^3 = a^2a = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$,

$a^4 = a^3a = \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = I$.

Hence $a^5 = a^4a = Ia = a$.

Similarly, $a^6 = a^4a^2 = a^2$,

$a^7 = a^4a^3 = a^3$,

$a^8 = a^4a^4 = I$, and so on.

Thus the set $G = \{a, a^2, a^3, a^4\}$ is closed with respect to permutation multiplication. Multiplication is associative in the set. The identity in G is $a^4 = I$. The inverses of a, a^2, a^3, a^4 are respectively a^3, a^2, a, a^4.

Also all the elements of G are integral powers of a. Hence it forms a cyclic group.

Ex. 7. *Show that the set* $\{1,-1,i,-i\}$ *forms a cyclic group for multiplication. Find its generator.* [K.H. 2001]

We have seen earlier that the set $\{1,-1,i,-i\}$ forms a group under arithmetical multiplication.

We see again that $(i)^1 = i, (i)^2 = -1, i^3 = -i$ and $i^4 = 1$.

Thus we see that it is a cyclic group whose generator is i.

Again $i^{-1} = -i$. Therefore $(-i)$is also a generator. This can be verified as $(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i$ and $(-i)^4 = 1$.

Ex. 8. *Show that every proper sub-group of an infinite cyclic group is infinite.*

Let $G = \{a\}$ be an infinite cyclic group. Suppose H is a proper sub-group of G. Now H is cyclic and if n be a positive integer such that $a^n \in H$, then a^n is a generator of H.

We suppose that H is a finite group of order p. Then

$$(a^n)^p = e, \text{ that is, } a^{np} = e.$$

This means that $o(a)$ is finite, which implies G is finite.

But this is a contradiction. Hence H must be infinite cyclic sub-group of G.

Ex. 9. *Show that every group of prime order is cyclic.* [C.H. 1996]

Let G be a finite group, whose order is a prime number p. Thus $p \neq 0, p \neq \pm 1$ and the only divisors of p are (± 1) and $(\pm p)$.

Since G is a group of prime order, so G must contain at least 2 elements; 2 is the least positive prime integer. Thus there is an element $a \in G$, such that it is not the identity element e.

Since a is not the identity element, therefore $o(a)$ must be ≥ 2.

Suppose $o(a)=m$; then $H = \{a\}$ is a cyclic sub-group of G and

$$o(H) = o(a) = m.$$

By Lagrange's theorem, m must be a divisor of p. But p is prime and $m \geq 2$. Therefore $m = p$. Hence $H = G$. Now H is cyclic.

Therefore G is cyclic and $G = \{a.\}$

Ex. 10. *Show that if the two right cosets Ha and Hb be distinct, then the two left cosets* $a^{-1}H$ *and* $b^{-1}H$ *are distinct.*

Here Ha and Hb are distinct.

If possible, let $a^{-1}H = b^{-1}H$.

Now $a^{-1}H = b^{-1}H \Rightarrow a^{-1} \in b^{-1}H$

$\Rightarrow ba^{-1} \in bb^{-1}H = eH = H$

$\Rightarrow \left(ba^{-1}\right)^{-1} \in H$, since H is a sub-group

$\Rightarrow ab^{-1} \in H$

$\Rightarrow Ha = Hb$.

But this contradicts our assumption.

Hence $a^{-1}H$ and $b^{-1}H$ are distinct.

Note. The converse of this result is also true and can be proved similarly.

Ex. 11. *Find the permutation group isomorphic to the group* $\{1,-1,i,-i\}$, *where* $i = \sqrt{-1}$.

If the required group be $\{\theta_1, \theta_{-1}, \theta_i, \theta_{-i}\}$, then

$$\theta_1 = \begin{pmatrix} 1 & -1 & i & -i \\ 1.1 & 1.(-1) & 1.i & 1.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix},$$

$$\theta_{-1} = \begin{pmatrix} 1 & -1 & i & -i \\ -1.1 & -1.(-1) & -1.i & -1.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix},$$

$$\theta_i = \begin{pmatrix} 1 & -1 & i & -i \\ i.1 & i.(-1) & i.i & i.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}$$

and $\theta_{-i} = \begin{pmatrix} 1 & -1 & i & -i \\ -i.1 & -i.(-1) & -i.i & -i.(-i) \end{pmatrix} = \begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}$.

Ex. 12. *If* G *and* G' *be two groups whose orders are* 10 *and* 6 *respectively, then show that there does not exist a homomorphism of* G *onto* G'.

If possible, let $\phi : G \to G'$ be an onto homomorphism.

Let K be the kernel of the homomorphism ϕ. Then, by the first theorem of isomorphism, the factor group G/K and the group G' are isomorphic.

Hence $o(G/K) = o(G') = 6$.

Since G is a finite group, $o(G/K) = o(G)/o(K)$.

So $6 = o(G)/o(K)$.

Hence $6\,o(K) = 10$, which is not possible.

Therefore the homomorphism ϕ does not exist.

Examples III (C)

1. If a be an element of a group G such that $a^2 = a$, then show that $a = e$.

2. If G be a group of even order, then prove that it has an element $a \neq e$, such that $a^2 = e$.

3. If a be an element of a group, then prove that the integral powers of a form a multiplicative group.

4. (a) If the elements a, b and ab of a group be each of order 2, then prove that $ab = ba$.

(b) If a be an element of order n of a group G and p be prime to n, then show that $o\left(a^p\right) = n$.

(c) In a group $(G, \bullet)$, the elements a and b commute and $o(a)$ and $o(b)$ are prime to each other. Show that $o(a.\,b) = o(a).o(b)$.

(d) If the elements a, b of a group commute, then prove that $(ab)^2 = a^2b^2$.

5. If a group G has four elements, then show that it must be abelian.

6.(a) Prove that a group is abelian, if every element of the group (except the identity) be of order two.

(b) From the result $\left(a^{-1}\right)^{-1} = a$, where $a \in G$, a group, show that every group of even order contains an element of order 2.

7. (a) Prove that if G be an abelian group and $a, b \in G$, then $(ab)^n = a^n b^n$ for all integers n.

(b) If G be a group such that $(ab)^m = a^m b^m$ for three consecutive integers m and for all $a, b \in G$, then show that G is abelian.

8. (a) Show that the set $H = \{1, -1\}$ is a sub-group of the multiplicative group $G = \{1, -1, i, -i\}$, when $i = \sqrt{-1}$.

(b) Show that the set of all 2×2 real matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ is a sub-group of the group of all 2×2 non-singular real matrices.

9. (a) In a group, if $ba = a^m b^n$, then prove that the elements $a^m b^{n-2}$, $a^{m-2}b^n$ and ab^{-1} have the same order.

(*b*) Let G be a group and $a, b \in G$. If $a^3 = e$ and $aba^{-1} = b^2$, then show that the order of b is 7.

[Here $(aba^{-1})^2 = ab^2a^{-1} = a(aba^{-1})a^{-1} = a^2ba^{-2}$

$\Rightarrow (aba^{-1})^4 = (a^2ba^{-2})(a^2ba^{-2}) = a^2b^2a^{-2} = a^2(aba^{-1})a^{-2} = a^3ba^{-3} = ebe = b$

$\Rightarrow b^8 = b$, giving $b^7 = e$.]

(*c*) Let a be an element of a group. If the order of a be 30, then show that the order of a^{18} is 5.

[Here $a^{30} = e \Rightarrow a^{90} = e \Rightarrow (a^{18})^5 = e$.]

10.(*a*) If a, b be two elements of a group such that $b^2ab = a^{-1}$, then show that $(ab)^3 = a$. [*C.H. 1993*]

Show further that $b^{-1}a^{-2}b = (b^{-1}ab)^{-2}$. [*C.H. 1996*]

(*b*) If, in a group G with identity element 1, $a, b \in G$ such that $a^4 = 1$ and $ab = ba^2$, then prove that $a = 1$. [*C.H. 1995*]

[Here $a^4 = 1 \Rightarrow ba^4 = b \Rightarrow aba^2 = b \Rightarrow a^2b = b \Rightarrow ab = b$.]

(*c*) Let a, b, c be three elements of a group G. If an element x of G satisfies $(axb)^{-1} = c^{-1}b^{-1}$, then show that $x = a^{-1}bcb^{-1}$.

11.(*a*) Prove that the group G is abelian, iff

$$(ab)^{-1} = a^{-1}b^{-1} \ \forall \ a, b \in G.$$

(*b*) Let G be a group. If $a^{-1}b^2(bab)^{-1}ba^2 = b \ \forall \ a, b \in G$, then show that G is a commutative group. [*C.H. 2003*]

$[a^{-1}b^2(bab)^{-1}ba^2 = b \Rightarrow a^{-1}b^2(b^{-1}a^{-1}b^{-1})ba^2 = b$

$\Rightarrow a^{-1}b\,a^{-1}a^2 = b \Rightarrow ba = ab$.]

12. Let a be an element of the group G. If $o(a)$ be infinite and p be a positive integer, then prove that $o(a^p)$ is infinite.

Show further that if $o(a)$ be infinite and p be a negative integer, then $o(a^p)$ is infinite.

13. Show that the order of each element of the group $[\{0, 1, 2, 3, 4\}, +5]$ is 5 and $o(0) = 1$.

14.(*a*) Let a be an element of a group G. Then show that the set $H = \{a^n : n \in I\}$ of all integral powers of a is a sub-group of G.

(*b*) Prove that every non-commutative group of order 6 must have a sub-group of order 3. [B.H. 2002]

(*c*) Show that the dihedral group of order 6 does not have a sub-group of order 4. [B.H. 2002]

15. G is a group of integers under addition. H is the sub-set consisting of all the multiples of 5. Show that H is a sub-group.

16. Let H be a sub-group of a group G. If $g \in G$, then show that $T = \{ghg^{-1} : h \in H\}$ is a sub-group of G. [C.H. 1987; V.H. 1998]

17.(*a*) In a group G, prove that the sub-set

$$A = \{a \in G : ag = ga \text{ for all } g \in G\}$$

is a sub-group of G. [C.H. 1991]

(*b*) If H and K be sub-groups of a commutative group G, then show that HK is a sub-group of G.

18.(*a*) Let H be a sub-group of a group G and a be an element of G.

Let $aH = \{ah : h \in H\}$. Prove that

(*i*) $a \in aH$;

(*ii*) for $b \in G$, if $b \notin aH$, then $aH \cap bH = \phi$. [C.H. 1991]

(*b*) Let H be a sub-group of a group G. A relation ρ on the set is defined by

$$\rho = \{(a,b) \in G \times G \mid a^{-1}b \in H\}.$$

Prove that ρ is an equivalence relation on G. [C.H. 1999]

(*c*) If $a^{-1}b \in H$, then show that $aH = bH$, where H is a sub-group of a group G and $a, b \in G$. [K.H. 2009]

19.(*a*) Show that the group G given by the set

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

is abelian with respect to matrix multiplication without being cyclic.

(*b*) Show that the set of even permutations of (1 2 3) is a cyclic group with respect to product of permutations. [C.H. 2004]

20. Prove that a cyclic group with only one generator can have at most two elements.

21. (*a*) Show that the set $\{1, \omega, \omega^2\}$ forms a multiplicative cyclic group, whose generators are ω and ω^2.

(*b*) Show that the additive group $G = [\{0, 1, 2, 3, 4, 5\}, +6]$ is cyclic with 1 and 5 as the generators.

(*c*) Show that the multiplicative group $G = [\{1, 2, 3, 4\}, \times 5]$ is cyclic with 2 and 3 as the generators.

(*d*) Show that the right coset of the sub-group $\{-1, 1\}$ of the multiplicative group of all non-zero reals that contain 5 is $(-5, 5)$.

22. Show that the set of all the n-th roots of unity forms a finite abelian group of order n for multiplication. Show further that it is a cyclic group generated by $e^{\frac{2\pi i}{n}}$.

23. (*a*) Show that any group G of order three is cyclic.

(*b*) Show that any group G of order 77 is cyclic.

24. Show that there are three generators of the cyclic group G of order eight and there are four generators of a cyclic group of order twelve.

25. Show that the group given by the following table is cyclic :

$\bullet$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

26. Show that the Klein 4-group formed of the finite set $\{1, a, b, c\}$ has three proper sub-groups $\{1, a\}$, $\{1, b\}$ and $\{1, c\}$.

Show further, from the composition table, that $\{1, a, b\}$ is not a sub-group.

Verify that the group is not cyclic.

27. If G be of finite order n, then show that the order of any $a \in G$ divides the order of G.

28. Show that every finite group of order less than six must be abelian.

29. If a finite group of order n contains an element of order n, then show that the group must be cyclic.

30. (*a*) Show that every proper sub-group of the symmetric group S_3 is cyclic. [*C.H. 1989, 1993*]

(*b*) In the symmetric group S_3, show that the sub-sets $A = \{e, (1\ 2)\}$ and $B = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$ are sub-groups.

Use Lagrange's theorem to show that $A \cup B$ is not a sub-group of S_3.

[Here the order of S_3 is 6 ; $A \cup B$ is a set of 4 elements but 4 is not a factor of 6.]

31. Show that the commutative group $\{Q, +\}$ of rational numbers under addition is a non-cyclic group.

Show further that $\{R, +\}$ is a non-cyclic group. [C.H. 1999]

32. If G be a cyclic group of prime order, then show that G has no proper sub-group. [K.H. 2009]

33. Prove that the centre of a group is always a normal sub-group.

34.(*a*) Prove that the set of matrices

$$S = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

forms a normal sub-group of the group

$$G = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \Big/ a, b \in R \text{ and } ab \neq 0 \right\}. \quad [V.H.\ 1998]$$

(*b*) A sub-group H of a group G has the property that $x^2 = H \ \forall x \in G$. Prove that H is normal in G and G/H is abelian. [V.H. 2009]

$[\, x \in G, h \in H \Rightarrow xhx^{-1} = xh\left(xhh^{-1}x^{-1}\right)x^{-1} = (xh)^2 h^{-1}\left(x^{-1}\right)^2 \in H\,.]$

35. Prove that an infinite cyclic group is isomorphic to the group (Z, +). [C.H. 2006]

36. (*a*) If $f : G \to H$ and $g : H \to K$ be given homomorphisms for the three groups H, G and K, then prove that gof is a homomorphism.

(*b*) If (G, o) be a group and a mapping $\phi : G \to G$ be defined by $\phi(x) = x^2, x \in G$, then prove that ϕ is a homomorphism, if and only if G be commutative.

(*c*) Let Z be the additive group of all integers and G be a multiplicative infinite cyclic group with generator a. Let the mapping $f : Z \to G$ be defined by $f(n) = a^n$. Prove that f is a homomorphism. [C.H. 1994]

4 RING AND FIELD

4.1. Introduction.

Group is an algebraic structure with one binary operation. In this chapter, we propose to study algebraic structures equipped with two binary operations. The two compositions are called addition and multiplication, being denoted by the ordinary notations, although they may not be ordinary addition and multiplication but well-defined compositions satisfying the necessary postulates.

4.2. Rings.

The simplest of the aforesaid systems is the ring as defined below :

A set of elements $a, b, c, \ldots\ldots$ forms a *ring* R with respect to the binary compositions — addition $(+)$ and multiplication $(\bullet)$ defined on R, if

(*i*) $a+b \in R$, for any two elements $a, b \in R$;

(*ii*) $a+(b+c)=(a+b)+c$, for any three elements $a, b, c \in R$;

(*iii*) there exists an element denoted by 0 in R such that

$$a+0=a, \text{ for all } a \in R;$$

(*iv*) for each element $a \in R$, there exists an element denoted by $(-a)$ in R such that $a+(-a)=0$;

(*v*) $a+b=b+a$, for any two elements $a, b \in R$;

(*vi*) $a.b \in R$, for any two elements $a, b \in R$;

(*vii*) $a.(b.c)=(a.b).c$, for any three elements $a, b, c \in R$;

(*viii*) $a.(b+c)=a.b+a.c$ and $(b+c).a=b.a+c.a$, for any three elements $a, b, c \in R$.

This algebraic structure is often written as $(R, +, \bullet)$ or $< R, +, \bullet >$, where R is the non-empty set of the ring. When the operations $+$ and $\bullet$ are defined, the set R defines a ring.

The first five conditions ensure that $(R, +)$ is a commutative group ; conditions (*vi*) and (*vii*) imply that $(R, \bullet)$ is a semi-group ; condition (*viii*) asserts the right as well as left distributive laws.

A ring R, in which multiplication is commutative, is called a *commutative* ring. For a communtative ring R,

$$a.b=b.a, \text{ for all } a, b \in R.$$

The set of all integers with two binary operations, addition and multiplication, forms a ring.

The set of real numbers, the set of rational numbers, the set of complex numbers, all form rings under usual addition and multiplication.

Cor. Since the ring is a group with respect to addition, all the group properties hold for addition.

The unique identity of the additive group, denoted by the ordinary symbol for the number zero, is called the *zero element* of the ring and is denoted by 0.

Thus $a+0=0+a=a$, for every a in the ring.

The unique additive inverse of an element a is denoted by $(-a)$, such that $a+(-a)=0=(-a)+a$.

For the additive operation, the left as well as right cancellation law holds good in a ring, that is, for all $a,b,c \in R$,

$a+b=a+c$ implies $b=c$

and $b+a=c+a$ implies $b=c$.

There will be a unique solution $x=b+(-a)$, written as $(b-a)$, of the equation $a+x=b$.

4.3. Some elementary properties of a ring.

(a) If the system $(R, +, \bullet)$ be a ring and $a \in R$ and 0 be the additive identity of the ring R, then

$$a.0=0, \quad 0.a=0.$$

We have $a.0+a.a=a.(0+a)$, right distributive law

$$=a.a, \text{ since } 0+a=a$$

$$=0+a.a.$$

Hence, by the right cancellation law,

$$a.0=0.$$

Similarly, by using the left distributive law, we can show that

$$0.a=0.$$

(b) If the system $(R, +, \bullet)$ be a ring with 0 as the additive identity and $a,b \in R$, then

$$a.(-b)=-(a.b), (-a).b=-(a.b) \text{ and } -(a).(-b)=a.b.$$

We have

$a.(-b+b)=a.(-b)+a.b$, right distributive law

$\Rightarrow a.0=a.(-b)+a.b$, $(-b)$ is the additive inverse of b

$\Rightarrow 0=a.(-b)+a.b$, from property (a).

Therefore $a.(-b)$ is an additive inverse of $a.b$.

Hence $a.(-b) = -(a.b)$.

Similarly, by using the left distributive law, we can easily show that

$$(-a).b = -(a.b).$$

From these two results, we have

$$(-a).(-b) = -\left[(-a).b\right] = -\left[-(a.b)\right] = a.b,$$

since the inverse of the inverse of an element is the element itself.

(c) *If the system* $(R, +, \bullet)$ *be a ring and* $a, b, c \in R$,

then $a.(b-c) = a.b - a.c$

and $(b-c).a = b.a - c.a$.

We have $a.(b-c) = a.\left[b+(-c)\right]$

$= a.b + a.(-c)$, right distributive law

$= a.b + [-(a.c)]$

$= a.b - a.c.$

Similarly, using the left distributive law, we can show that

$$(b-c).a = b.a - c.a.$$

4.4. Ring with unity.

If a ring R contains an element u such that

$$u.a = a.u = a,$$

for every $a \in R$, then u is called the *unity element*. It is generally denoted by u or the number 1.

Thus a ring R is said to be a *ring with unity*, if R has a multiplicative identity, that is, if there exists an element 1 in R, such that

$$1.a = a.1 = a, \text{ for every } a \in R.$$

R may or may not contain a multiplicative identity.

The set of all integers is a ring under usual addition and multiplication and moreover it has the multiplicative identity 1. Hence it is a ring with unity. Similarly, the set of all real numbers is a ring with unity element. But the set of even integers $2Z$ is a commutative ring without unity under the same operations.

If R be a ring with unity 1, then an element $a \in R$ is called a *unit*, if there exists an element b in R such that $a.b = 1 = b.a$. We write $b = a^{-1}$ and call it a *multiplicative inverse* of a.

The set R consisting of a single element 0 with two binary operations defined by

$$0 + 0 = 0 \quad \text{and} \quad 0.0 = 0$$

is a ring, called the *null ring* or a *trivial ring*. In this ring, 0 is the additive as well as the multiplicative identity.

In a non-trivial ring R, there exists a non-zero element in R.

Theorem 1. *If R be a ring with unity 1, then this is the unique multiplicative identity.*

If possible, let there be two multipliative identities 1 and $1'$.

Then, by definition,

$1.a = a.1 = a$ and $1'.a = a.1' = a$, for all a in R.

Now, 1 and $1'$ being multiplicative identities,

$$1.1' = 1'$$
$$= 1.$$

Therefore $1 = 1'$.

Thus the multiplicative identity is unique.

Theorem 2. *If R be a non-trivial ring with unity 1, then $1 \neq 0$ in R.*

Since R is non-trival, there exists an element $a \neq 0$ in R. Let, if possible, $1 = 0$. Then $a.1 = a.0$ and this implies $a = 0$. This contradicts the assumption and hence $1 \neq 0$ in R.

4.5. Powers and integral multiples of an element of a ring.

Every ring is a multiplicative semi-group. Hence the powers a^n (n being any positive integer) may be defined for every element a of the ring and we have the following properties :

$$(i)\ a^m.a^n = a^{m+n}, \quad (ii)\ \left(a^m\right)^n = a^{mn}, \quad (iii)\ (ab)^m = a^m b^m.$$

The property (*iii*) holds for commutative ring.

Again, let R be a ring and $a \in R$. If m be a positive integer, then we define

$$ma = a + a + a + \ldots\ldots \text{ to } m \text{ terms.}$$

Again, by definition, we have $0a = 0$. Here 0 on the left is the integer 0 and 0 on the right is the additive identity of R. If m be a positive integer, then $(-m)$ is a negative integer. We define

$$(-m)\,a = -(ma) = -(a + a + a + \ldots\ldots \text{ to } m \text{ terms})$$
$$= (-a) + (-a) + \ldots\ldots \text{ to } m \text{ terms}$$
$$= m\,(-a).$$

In this connection, we have the following properties :

If R be a ring and m, n be any positive integers, then

(*i*) $(m+n)a = ma + na \quad \forall a \in R$,

(*ii*) $m(a+b) = ma + mb \quad \forall a, b \in R$,

(*iii*) $m(na) = (mn)a \quad \forall a \in R$.

4.6. Characteristic of a ring.

The *characteristic* of a ring R is the smallest positive integer m, if it exists, such that $ma = 0$, for all $a \in R$.

Here ma means $a + a + \ldots\ldots + a$ (m terms).

If no such m exists, then the characteristic of R is said to be zero.

The characteristic of the ring $(Z, +, \cdot)$ is zero.

The characteristic of the ring of integers, with addition and multiplication modulo n, is n.

Theorem. *If R be a ring with unity 1, then R is of characteristic n (> 0) iff $n\,1 = 0$ and n is the smallest positive integer.*

If R has characteristic $n > 0$, then, from definition, we have, for all $a \in R$, $na = 0$. In particular, $n\,1 = 0$. Conversely, let n be the smallest positive integer, such that $n\,1 = 0$. Then, for any $a \in R$, we have

$$\begin{aligned} na &= a + a + \ldots\ldots + a \quad (n \text{ terms}) \\ &= a\,(1 + 1 + \ldots\ldots \text{ upto } n \text{ terms}) \\ &= a.\, n\,1 = a.\, 0 = 0. \end{aligned}$$

Hence R has characteristic n.

4.7. Rings with zero divisors.

Let R be a ring. If the non-zero elements $a, b \in R$ be such that

$$a.b = 0 \quad \text{or} \quad b.a = 0,$$

then a and b are called *divisors of zero* (or *zero divisors*).

In the former case, a is said to be the left divisor of zero and in the latter case, a is said to be the right divisor of zero.

If, however, R be a commutative ring, then every left divisor of zero is also a right divisor of zero.

A ring R is said to be *without zero divisors*, if the product of no two non-zero elements of the same be zero, that is,

$$a.b = 0 \Rightarrow \text{either } a = 0 \text{ or } b = 0$$
$$\text{or both } a = 0 \text{ and } b = 0.$$

In the alternative case, R possesses zero divisors.

The ring of integers is without zero divisors, since the product of two non-zero integers cannot be equal to zero. The rings $(Q, +, \cdot)$ and $(R, +, \cdot)$ contain no divisor of zero. But a ring of integers with addition and multiplication modulo 6 is a ring with zero divisors, since

$$[2 \times 3 \pmod 6] = 0 \text{ but } 2, 3 \neq 0.$$

Again, let M be a ring of all 2×2 matrices with their elements

$A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ as two non-zero elements.

We have

$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ = the null matrix, which is the zero element of the ring.

Hence M is a ring with zero divisors.

Furthermore we have

$$BA = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Thus, in a ring R, it is possible that $ab = 0$ but $ba \neq 0$.

An element a of a ring is called *nilpotent*, if there exists some positive integer n, such that $a^n = 0$. A nilpotent element $a \neq 0$ is a divisor of zero.

In the ring M, there is an element $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ which is nilpotent, since

$$\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}^2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

In a non-trivial ring R with unity, an element $a \in R$ is said to be a *unit*, if there exists an element b in R, such that $a.b = b.a = 1$, 1 being the unity in R.

b is called the *multiplicative inverse* of a and is denoted by a^{-1}.

If a be a unit in the ring R, then $a.a^{-1} = a^{-1}.a = 1$.

1 and (-1) are the only units in the ring $(Z, +, \cdot)$ and each non-zero element is a unit in the ring $(Q, +, \cdot)$.

A ring $(R, +, \cdot)$ is said to be a *Boolean ring*, if $a^2 = a$, for all a in R.

$\{0, 1\}$ is a Boolean ring under usual addition and multiplication.

4.8. Cancellation laws in a ring.

If $a, b, c \in R$ and if in R

$$a.b = a.c\,(a \neq 0) \Rightarrow b = c$$

and $$b.a = c.a\,(a \neq 0) \Rightarrow b = c,$$

then we say that the cancellation laws hold in the ring R.

Now, if the ring be with zero divisors, then the cancellation laws do not hold in it. In such a ring, $a.b = 0$ does not imply either a or b is zero or both a and b are zero.

Theorem 1. *A ring R has no divisors of zero, if and only if the cancellation laws hold in R.*

Let a, b, c be three elements of R, which has no divisors of zero, so that

$$a.b = a.c,\ a \neq 0.$$

Now $a.b = a.c$ implies $a.(b-c) = 0$.

Since $a \neq 0$ and R has no divisors of zero, we have

$b - c = 0$, that is, $b = c$,

which establishes the left cancellation law in R. Similarly, one can show that the right cancellation law also holds in R.

On the other hand, if we assume that the cancellation laws hold in R and if possible,

let $a.b = 0,\ a \neq 0,\ b \neq 0,$

then $a.b = a.0$, since $a\,0 = 0$,

so that, by the left cancellation law, we have $b = 0$, which contradicts our assumption.

Hence R has no divisors of zero.

Theorem 2. *If a be a unit in a ring R, then a is not a divisor of zero.*

Let $b \in R$ be such that $a \,.\, b = 0$.

Since a is a unit, therefore a^{-1} exists in R.

Thus we have $a^{-1}.(a.b) = a^{-1}.0 = 0$

or, $(a^{-1}.\ a).b = 0$

or, $1.b = 0$, that is, $b = 0$, (1 is the unity element).

Let $c \in R$ be such that $c.a = 0$.

Then we have $(c.a).a^{-1} = 0.a^{-1} = 0$,

that is, $c.(a.a^{-1}) = c.1 = 0$; hence $c = 0$.

Thus a is not a left or right divisor of zero.

Theorem 3. *In a ring R with unit a, the multiplicative inverse is unique.*

If possible, let b and c be two multiplicative inverses of a, so that $a.b = b.a = 1$ and $a.c = c.a = 1$, 1 being the unity of R.

Now $b.(a.c) = (b.a).c$, multiplication being associative,

that is, $b.1 = 1.c$, which implies $b = c$.

Thus the multiplicative inverse is unique.

Theorem 4. *In a non-trivial ring R with unity, the zero element has no multiplicative inverse.*

If possible, let 0 be a unit in R.

Then there exists an element $b \in R$, such that

$$0.b = b.0 = 1,$$ 1 being the unity in R.

But we have $0.b = b.0 = 0$, which contradicts the assumption.

4.9. Sub-rings.

Let $(R, +, \cdot)$ be a ring. Any non-empty sub-set S, of the set R, is said to be a *sub-ring* of R, if S be closed with respect to the operations of addition and multiplication and S be itself a ring with respect to these operations.

The set of all integers forms a sub-ring of the set of all rational numbers.

The set of even integers is a sub-ring of the ring of integers, although the former has no unity and the latter has unity.

$(Z, +, \cdot)$ is a sub-ring of the ring $(Q, +, \cdot)$ having the same unity.

If S be a sub-ring of a ring R, then it is obvious that S is a sub-group of the additive group R and a semi-group of the multiplicative semi-group R.

The zero element of R forms a ring by itself. It is said to be the *trivial sub-ring* of R.

Furthermore, if R be a ring, then $\{0\}$ and the set R are always sub-rings of the ring R (*improper sub-rings*). Any other sub-ring of R that may exist is called a *proper sub-ring*.

Theorem 1. *A non-empty sub-set S of a ring $(R, +, \cdot)$ will form a sub-ring of R, if and only if, for any two elements x and y of S,*

$$x - y \text{ and } x.y \in S, \text{ for all } x, y \in S.$$

Let $(S, +, \cdot)$ be a sub-ring of $(R, +, \cdot)$; then $(S, +)$ is an additive sub-group of $(R, +)$, so that

$$y \in S \Rightarrow -y \in S$$

and $$x - y = x + (-y) \in S.$$

Again, S, being a sub-ring, is closed under multiplication so that we have $x \in S$ and $y \in S \Rightarrow x.y \in S$.

Conversely, let $x \in S$ and $y \in S \Rightarrow x-y \in S$ and $x.y \in S$.

Then, since $(R, +)$ is an abelian group,

$$S \subseteq R \text{ and } x \in S, y \in S \Rightarrow x-y = x+(-y) \in S.$$

Therefore $(S, +)$ is an abelian sub-group of $(R, +)$. By hypothesis, S is closed under multiplication and since $S \subseteq R$, associativity with respect to multiplication must hold in S. Finally, the distributive laws hold in S, because these laws hold in R for all $x, y, z \in R$ and hence for all $x, y, z \in S$.

Hence $(S, +, \bullet)$ is a ring.

Theorem 2. *The intersection of two sub-rings is a sub-ring.*

Let S and T be two sub-rings of a ring $(R, +, \bullet)$.

We shall show that $S \cap T$ is also a sub-ring of $(R, +, \bullet)$.

Let $x, y \in S \cap T$. Then $x, y \in S$ and $x, y \in T$. But, since S and T are sub-rings, by the theorem 1,

$$x-y \in S \text{ and } x.y \in S.$$

Also $$x-y \in T \text{ and } x.y \in T.$$

Therefore $x-y \in S \cap T$ and $x.y \in S \cap T$.

Hence $S \cap T$ is a sub-ring.

Note. Union of two sub-rings of a given ring may not be a sub-ring.

4.10. Illustrative Examples.

Ex. 1. *If Z be a set of integers, positive, negative and zero, then show that Z forms a commutative ring with unity for ordinary addition and multiplication.*

We have $Z = \{\ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots\}$.

We observe that, for any $a, b, c \in Z$,

(i) $a \in Z, b \in Z$ imply $a+b \in Z$ (closure);

(ii) $a+(b+c) = (a+b)+c$ (associative);

(iii) $a+0 = 0+a = a$ (identity);

(iv) $a+(-a) = (-a)+a = 0$ (inverse);

(v) $a+b = b+a$ (commutative).

Therefore Z forms an abelian group for addition (+).

Again we see that

(*vi*) $(a.b).c = a.(b.c)$ (multiplication is associative);

(*vii*) $a.b \in Z$ (closed for multiplication);

(*viii*) $a.(b+c) = a.b + a.c$ (right distributive law),

$(b+c).a = b.a + c.a$ (left distributive law).

Further $a.b = b.a$ (commutative law for multiplication).

Therefore Z is a commutative ring.

Again $1.a = a.1 = a$, for all $a \in R$.

Therefore Z forms a commutative ring with unity.

Ex. 2. (*a*) *Let R be a ring with unity element* 1, *then show that*

(*i*) $(-1)a = -a = a(-1)$, *for all* $a \in R$,

(*ii*) $(-1)(-1) = 1$.

(*b*) *Show that the equation* $a + x = b$ *has a unique solution in a ring R.*

(*a*) (*i*) We have, by the distributive laws in a ring,

$$(-1+1)a = (-1)a + 1.a,$$

that is, $0.a = (-1)a + a$,

that is, $(-1)a = -a$. ... (1)

Again $a(-1+1) = a(-1) + a.1$,

that is, $a.0 = a(-1) + a$, that is, $0 = a(-1) + a$,

that is, $a(-1) = -a$. ... (2)

From (1) and (2), we have $(-1)a = -a = a(-1)$. ... (3)

(*ii*) Putting $a = -1$ in (3), we have

$$(-1)(-1) = -(-1) = (-1)(-1).$$

We know that $-(-x) = x$ in an additive group.

Therefore $-(-1) = 1$.

Hence we get $(-1)(-1) = 1$.

(*b*) We have $a + (b-a) = a + (-a+b)$

$$= (a-a) + b = 0 + b = b.$$

Thus $(b-a)$ is a solution of $a + x = b$.

If possible, let c be another solution of $a+x=b$.
Then $a+c=b$. So $a+c=a+(b-a)$. Therefore $c=b-a$.
This proves the uniqueness.

Ex. 3. *If R be a ring and $a,b,c\in R$, then show that*

(*i*) $-(a+b)=-a-b$,

(*ii*) $a-(b+c)=(a-b)-c$. [C.H. 1986]

(*i*) Let us prove that $(-a-b)$ is the inverse of $(a+b)$ with respect to 0.

We have $(a+b)+(-a-b)=a+\left[b+(-a-b)\right]$

$=a+\left[b+\{-b+(-a)\}\right]$

$=a+\left[b+(-b)+(-a)\right]$

$=a+\left[0+(-a)\right]$

$=a+(-a)$

$=0$.

Hence $-(a+b)=-a-b$.

(*ii*) We have $a-(b+c)=a+(-b-c)$, by (*i*)

$=a+\{-b+(-c)\}$

$=\{a+(-b)\}+(-c)$

$=(a-b)-c$.

Ex. 4. *If R be a ring such that $a^2=a$, for all $a\in R$, then prove that*

(*i*) $a+a=0$, *for all* $a\in R$, [V.H. 1987]

(*ii*) $a+b=0\Rightarrow a=b$, [N.B.H. 1999]

(*iii*) $ab=ba$, *for all* $a,b\in R$ *(that is, R is a commutative ring).* [C.H. 1987]

Show further that the characteristic of R is 2. [V.H. 1998]

(*i*) We have $(a+a)=(a+a)^2=(a+a)(a+a)$

$=a(a+a)+a(a+a)$

$=(aa+aa)+(aa+aa)$

$=(a+a)+(a+a)$, since $a^2=a$

or, $0+(a+a)=(a+a)+(a+a)$.

Therefore, by the right cancellation law,

$$0 = a + a. \qquad \ldots (1)$$

(*ii*) Again, if $a + b = 0$, then, from (1), we have

$$a + b = a + a.$$

Therefore $b = a$, by the left cancellation law.

(*iii*) $(a+b) = (a+b)^2 = (a+b)(a+b)$

$$= a(a+b) + b(a+b)$$

$$= (aa + ab) + (ba + bb)$$

$$= (a + ab) + (ba + b), \quad \text{since } a^2 = a,\ b^2 = b$$

$$= (a + ab) + (b + ba)$$

$$= [(a + ab) + b] + ba$$

$$= [a + (ab + b)] + ba$$

$$= [a + (b + ab)] + ba$$

$$= [(a + b) + ab] + ba$$

$$= (a + b) + (ab + ba)$$

or, $$(a+b) + 0 = (a+b) + (ab + ba).$$

Therefore $0 = ab + ba$, by the left cancellation law.

Hence, by the result (*ii*), we get $ab = ba$.

Thus R is a commutative ring.

Furthermore, from (1), we have $2a = 0$.

Thus the characteristic of R is 2.

Ex. 5. *In the ring* $\{S, +, \cdot\}$, *S is a set of* 2×2 *matrices of the form* $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$, *where a, b, c are even integers and* $+$ *and* $\cdot$ *are respectively matrix addition and matrix multiplication. Show that* $\{S, +, \cdot\}$ *is a non-commutative ring with no unity element.* [T.H. 2009]

Let $A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$, where $A, B \in S$.

Check that the following hold :

(*i*) $A + B \in S$.

(*ii*) Addition is associative, since matrix addition obeys associative law.

(*iii*) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = O$ is the additive identity for S.

(*iv*) The matrix $\begin{bmatrix} -a_1 & -b_1 \\ 0 & -c_1 \end{bmatrix}$ belongs to S and is the additive inverse of A.

(*v*) $A + B = B + A$; hence $\{S, +\}$ is an abelian group under $+$.

(*vi*) $A.B \in S$, since the elements of A, B are all even integers.

(*vii*) Multiplication is associative, since matrix multiplication always obeys associative law.

(*viii*) The left and the right distributive laws hold in S.

Hence $\{S, +, \cdot\}$ is a ring.

(*ix*) In general, $A.B \neq B.A$. Hence the ring is non-commutative.

To prove that the ring has no unity element, let

$$C = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix}, \text{ where } x, y, z \text{ are even and } C \in S.$$

If C be a unity element for S, then we should have $AC = A$,

that is, $\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}\begin{bmatrix} x & y \\ 0 & z \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$,

that is, $\begin{bmatrix} a_1 x & a_1 y + b_1 z \\ 0 & c_1 z \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$.

Hence, for all even integers a_1, b_1, c_1, we must have

$$x = 1, y = 0, z = 1.$$

Since x and z must be even, the ring has no unity element.

Ex. 6. *Show that the set of matrices of the form* $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ *is a sub-ring of all* 2×2 *matrices over the set of real numbers.*

We have

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} - \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 - a_2 & b_1 - b_2 \\ 0 & c_1 - c_2 \end{bmatrix}$$

and

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix}.$$

Thus the difference and product of two matrices of the form

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

are again of the same form. Hence the result follows.

Examples IV(A)

1. Show that the set of rational numbers forms a commutative ring with unity element with respect to ordinary addition and multiplication.

2. Verify that each of the following sets forms ring under usual addition and multiplication :

(*i*) a set of even integers ;

(*ii*) a set of numbers of the form $3m$, with m an integer ;

(*iii*) a set of all numbers of the form $\left(a + b\sqrt{2}\right)$, $a, b \in Z$;

(*iv*) a set of all numbers of the form $\left(a + b\sqrt{2}\right)$, $a, b \in Q$;

(*v*) a set of all complex numbers of the form $(a + ib)$, $a, b \in Z$.

3. Verify that each of the following sets does not form ring under usual addition and multiplication :

(*i*) a set of natural numbers ;

(*ii*) a set of numbers of the form $b\sqrt{2}$, with b rational ;

(*iii*) a set of odd integers ;

(*iv*) a set of all purely imaginary numbers of the form ia, $a \in R$;

(*v*) a set of numbers of the form $\left(a + b\sqrt{2} + c\sqrt{3}\right)$ with a, b, c integral.

4. Show that the set of all square matrices $M_{2\times 2}$ over the field of real numbers is a non-commutative ring with unity under the operations of matrix addition and multiplication. [C.H. 1991]

5. Show that a set of all square matries of the form

(*i*) $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, a,b \in Z,$ (*ii*) $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a,b \in Q,$

(*iii*) $\begin{bmatrix} a & b \\ c & d \end{bmatrix}, a,b,c,d \in Q$

forms ring under the operations of matrix addition and multiplication.

6. Show that the ring M_2 of all 2×2 matrices $\begin{bmatrix} 2a & 0 \\ 0 & 2b \end{bmatrix}$ contains divisors of zero but does not contain the unity, if $a,b \in Z$.

7. Show that the ring M_2 of all 2×2 matrices $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ contains no divisor of zero if $a,b \in Q$, but contains divisors of zero if $a,b \in R$.

8. Let $M_2(R)$ denote the ring of all 2×2 matrices over the field of real numbers under usual matrix addition and multiplication. Show that this is a non-commutative ring with identity and with divisors of zero. [C.H. 1999]

9. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$, where a and b are real numbers, forms a non-commutative ring under usual matrix addition and multiplication.

10. (*a*) Prove that, in a ring R, for all $a,b \in R$,

(*i*) $-(-a) = a$; (*ii*) $a(-b) = (-a)b = -(ab)$; [C.H. 1989; V.H.1997]

(*iii*) $(ma)(nb) = (mn)ab$, m and n being positive integers.

(*b*) For any two elements x, y of a ring, prove that $(-x)(-y) = xy$.

11. In a ring R, prove that $(a-b)-c = a-(b+c)$, for all $a,b,c \in R$. [K.H. 1982; C.H. 1996]

12. If, in a ring R, $a+c = b+c$, then show that $a = b$, where $a,b,c \in R$.

13. If $a^2 = a$, for every element a in a ring R, then show that $b = -b$, for every $b \in R$. [C.H. 1989; 199?]

Show further that R is commutative. [C.H. 1994]

14. Show that R is a commutative ring, if $x^3 = x$, for all $x \in R$.

15. (*a*) If, in a ring $\{R, +, \bullet\}$, an element $a \in R$ has a multiplicative inverse $a^{-1} \in R$, then prove that it is unique.

(*b*) In a ring with identity, if a^{-1} and b^{-1} exist, then prove that $(a \bullet b)^{-1}$ exists. [*B.H. 1998*]

$[(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = 1.$

Hence $(ab)^{-1}$ exists and is equal to $b^{-1}a^{-1}$.]

16. If, in a ring R with identity and without divisors of zero, $ab = 1$, then prove that $ba = 1$. [*V.H. 1988*]

17. Prove that a ring R is commutative, iff

$$(a+b)^2 = a^2 + 2ab + b^2, \text{ for every } a, b \in R. \quad [C.H.\ 1992]$$

18. If R be a ring in which $x^2 = x$ for all x, then prove that

$$(a+b)^2 = a^2 + 2ab + b^2, \text{ for all } a, b \in R.$$

19. If a, b, c, d be elements of a ring R, then prove that

$$(a+b)(c-d) = ac + bc - ad - bd.$$

20. Show that the set of integers with the composition o and $*$ defined by

$$a \circ b = a + b - 1,$$
$$a * b = a + b - ab,$$

is a commutative ring, where $a, b \in Z$.

Show, further that 1 is the zero element and 0 is the unity.

21. (*a*) Show that the characteristic of the rings of the sets

(*i*) R, (*ii*) $2Z$, (*iii*) $M_2(R)$ is each equal to zero.

(*b*) If R and R' be rings such that $R = R'$, then prove that the characteristics of R and R' are the same.

22. Let a and b be arbitrary elements of a ring R whose characteristic is 2 and $ab = ba$. Then show that $(a+b)^2 = a^2 + b^2 = (a-b)^2$.

23. If $u \in R$, a ring be such that $u + a = a$ for all $a \in R$, then prove that $ua = au = u$, for all $a \in R$.

24. If, in a ring R with unity, an element x has an inverse with respect to multiplication, then show that, for $y \in R$,

$xy = 0$ implies $y = 0$.

25. Prove that the set $S = \{0, 1, 2, 3, 4\}$ is a ring with respect to the operations of addition and multiplication modulo 5.

26. In a finite non-trivial ring R, if a be not a divisor of zero, then show that a is a unit in R. Show that its converse is also true.

27. Show that the units in the ring R are all non-zero real numbers, those in Q are all non-zero rational numbers but those in Z are 1 and (–1).

28. If $(R, +, \cdot)$ be a ring such that $(R, +)$ is a cyclic group, then prove that the ring is commutative.

29. Prove that every finite Boolean ring contains 2^n elements for some natural number n.

30. Show that the set Z_n of the residue classes of integers modulo a given positive integer n forms a ring with respect to addition and multiplication of the classes.

31. Show that the sets of all of 2×2 real matrices of the form

$$(i)\ \begin{bmatrix} a & 0 \\ c & d \end{bmatrix} \text{ and } (ii)\ \begin{bmatrix} a & b \\ b & a \end{bmatrix}$$

are sub-rings of the ring of 2×2 matrices. But the sets of real matrices of the form

$$(iii)\ \begin{bmatrix} 0 & b \\ c & d \end{bmatrix} \text{ and } (iv)\ \begin{bmatrix} a & b \\ c & 0 \end{bmatrix}$$

do not form ring, where $a, b, c, d \in R$.

32. Show that the set of all matrices of the form

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix},$$

where a, b are integers, is a sub-ring of the ring of all 2×2 integral matrices under matrix addition and multiplication. [C.H. 1996]

33. a is a fixed element of the ring R.

Show that the set $S = \{x \in R : x.a = 0\}$ is a sub-ring of R.

[$x, y \in S$; hence $x.a = y.a = 0$.

$(x - y).a = x.a - y.a = 0$; hence $x - y \in S$.

$(x.y).a = x.(y.a) = x.0 = 0$; hence $x.y \in S$.]

34. R is a ring of integers. Let m be any fixed integer and let S be any sub-set of R, such that

$$S = \{\ldots\ldots, -3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots\}.$$

Show that S is a sub-ring of R.

35. Show that the set of numbers of the form $a + b\sqrt{2}, a, b \in Z$ is a sub-ring of the ring of real numbers.

36. The centre of a ring R is defined to be

$$\{a \in R : ax = xa \text{ for every } x \in R\}.$$

Show that the centre of a ring is a sub-ring.

4.11. Integral domains.

A ring containing at least two elements is called an *integral domain*, if it be commutative, it has unity and be without zero divisors.

The rings $(Z, +, \cdot)$, $(Q, +, \cdot)$, $(R, +, \cdot)$ are integral domains. The ring of even integers does not contain the unity element and hence it is not an integral domain, although it is without zero divisors . The set of natural numbers N does not form an integral domain. The ring $M_2(R)$ of all 2×2 matrices over the field of real numbers under usual matrix addition and multiplication is not an integral domain, since it is not commutative.

Note 1. Some authors do not demand a unity element for an integral domain.

Note 2. An integral domain is sometimes denoted by D.

Theorem 1. *A commutative ring R with unity is an integral domain, if and only if, for a non-zero element $a \in R$,*

$$a.b = a.c \Rightarrow b = c;\ b, c \in R.$$

Let $c = 0$; then, from the given condition,

$$a.b = a.0 \Rightarrow b = 0$$

or $$a.b = 0 \Rightarrow b = 0.$$

Thus a is not a left divisor of zero. R being a commutative ring, a is not a right divisor of zero too.

Thus R has no divisor of zero.

Hence R is an integral domain.

Conversely, let R be an integral domain and $a(\neq 0) \in R$.

Since R contains no divisor of zero, a is not a divisor of zero.

Therefore $a.b = a.c \Rightarrow a(b-c) = 0$

$\Rightarrow b - c = 0.$

Hence $b = c.$

Theorem 2. *The characteristic of an integral domain is either zero or a prime number.*

Let $(D, +, \cdot)$ be an integral domain having finite characteristic $n(\neq 0)$. Let us further assume that n is not a prime but a composite number and $n = rs$ for some integers r and s, such that

$$r < n \text{ and } s < n.$$

Since n is a characteristic of D,

$0 = n\,1$, 1 being the unity of D

$= rs\,1$

$= 1 + 1 + 1 + \cdots\cdots + 1$ (rs terms)

$= [1 + 1 + \cdots\cdots + 1 \text{ (r terms)}][1 + 1 + \cdots\cdots + 1 \text{ (s terms)}]$

$= (r1).(s1).$

Now, D being an integral domain, it must not contain divisors of zero. Hence either $r\,1 = 0$ or $s\,1 = 0$. But, since r and s are integers such that $r < n$ and $s < n$, either $r\,1 = 0$ or $s\,1 = 0$.

This gives that either r or s is the characteristic of D which contradicts the fact that n is the characteristic of D. This contradiction asserts that n is either zero or a prime number.

4.12. Fields.

Any ring, containing at least two elements, is called a *field*, if it be commutative, has a unity element and be such that all non-zero elements have multiplicative inverses.

Thus an integral domain is a field, if every element $a\ (\neq 0)$ has a multiplicative inverse a^{-1}, such that

$$a^{-1}.\ a = \text{ unity element.}$$

The ring of rational numbers is a field, since it is a commutative ring with unity and each non-zero element has a multiplicative inverse. The ring of all integers is not a field, since all non-zero elements in the ring of integers do not have multiplicative inverses.

Thus a set F having at least two elements which forms an algebraic structure $(F, +, \cdot)$ with the binary operations of addition and multiplication is called a field, if the following be satisfied :

(*i*) $a+b \in F$, whenever $a, b \in F$.

(*ii*) $a+(b+c)=(a+b)+c$, $a, b, c \in F$.

(*iii*) There exists an element $0 \in F$, such that
$a+0=0+a=a$ for all $a \in F$.

(*iv*) $a+b=b+a$.

(*v*) $a+x=b$ is solvable, for all $a, b \in F$.

(*vi*) $a.b \in F$, whenever $a, b \in F$.

(*vii*) $a.(b.c)=(a.b).c$, for all $a, b, c \in F$.

(*viii*) There exists an element $1 \in F$, such that
$a.1=1.a=a$, for all $a \in F$.

(*ix*) $a.b=b.a$, for all $a, b \in F$.

(*x*) $a.x=b$ is solvable, for all $a, b \in F$, where $a \neq 0$.

(*xi*) $a.(b+c)=a.b+a.c$, for all $a, b, c \in F$.

(*xii*) $(b+c).a=b.a+c.a$, for all $a, b, c \in F$.

It follows from (*x*) that, for every $a \in F$, $a \neq 0$, there exists an element $a^{-1} \in F$, such that $a^{-1}.a=a.a^{-1}=1$.

The rings $(Q, +, \cdot)$, $(R, +, \cdot)$ and $(C, +, \cdot)$ are examples of field.

The ring $(M_2(R), +, \cdot)$ is not a field, as multiplication in this system is not commutative.

Theorem 1. *Every field is an integral domain.*

To prove the theorem, we are to prove that in a field there exists no divisors of zero, that is, if F be a field and $a, b \in F$, then $a.b=0$ implies either $a=0$ or $b=0$.

If $a \neq 0$, then a^{-1} exists and we have, since $a.b=0$,

$$a^{-1}.(a.b)=a^{-1}.0.$$

Therefore $(a^{-1}.a).b=0$,

that is, $1.b=0$, since $a^{-1}.a=1$,

that is, $b=0$, since $1.b=b$.

Here 0 is the additive identity and 1 is the multiplicative identity.

Similarly, if $b \neq 0$, we can show that $a = 0$.

Thus the field, having no zero divisor, is an integral domain.

Note. The converse of this theorem is not true. The ring of integers is an integral domain but not a field.

Theorem 2. *A finite integral domain is a field.*

We know that an integral domain is a commutative ring with unity element. Let $(D, +, \cdot)$ be a finite integral domain consisting of n elements

$$a_1, a_2, a_3, \ldots\ldots, a_n$$

with unity element 1. Thus D has no zero divisor. To show that it is a field, we are to show that each non-zero element of D admits of a multiplicative inverse.

Now D contains a finite number of elements in which let a be a non-zero element. Now let us consider a set

$$D' = \{a.x : x \in D \text{ and } x \neq 0\}. \quad \ldots \quad (1)$$

Since the cancellation law holds in (1), we have

$$a.x = a.y \Rightarrow x = y.$$

From this, we see that all the elements of D' are distinct, the number of elements being $(n-1)$, since $x \neq 0$, and D' consists of non-zero elements of D. This shows that one of the elements of D' must be equal to the unity element 1, since $1 \neq 0$ in a non-trivial ring.

Thus, to each non-zero element a of D, there exists a non-zero element x of D, such that

$$a.x = 1 \text{ and so } x.a = 1,$$

that is, the multiplicative inverse of a is x.

This proves the theorem and D is a field.

Note. Since every field is an integral domain, the characteristic of a field is either 0 or a prime number.

4.13. Division ring or skew field.

A ring R with at least two elements is called a *division ring* (or *a skew field*), if

(*i*) it has unity,

(*ii*) each of its non-zero elements has a multiplicative inverse.

Theorem 1. *A skew field contains no divisor of zero.*

Let S be a skew field and $a, b \in S$ be such that

$$a.b = 0 \text{ and } a \neq 0.$$

Now each non-zero element of S is a unity, so a^{-1} exists in S.

Therefore $a^{-1}.(a.b) = a^{-1}.0 = 0$

or, $(a^{-1}.a).b = 0$

or, $1.b = 0$, that is, $b = 0$.

Thus a is not a left divisor of zero.

Similarly it can be shown that a is not a right divisor of zero.

Theorem 2. *The set of non-zero elements of a division ring forms a group under multiplication.*

If S^* be the set of non-zero elements of the skew field S and the non-zero elements $a, b \in S$, then since S contains no divisors of zero, we have $a.b \neq 0$.

Therefore $a, b \in S^*$ and S^* is closed with respect to multiplication.

S^* being a sub-set, multiplication is associative in S^*.

Now each non-zero element of S is a unity ; hence each element of S^* has a multiplicative inverse.

Hence $\{S^*, \bullet\}$ is a group.

4.14. Sub-fields.

If the system $(F, +, \bullet)$ be a field and F' be a sub-set of F such that $(F', +, \bullet)$ is also a field, then the system $(F', +, \bullet)$ is a *sub-field* of $(F, +, \bullet)$.

The set of rational numbers is a sub-field of the field of real numbers.

The set of real numbers is a sub-field of the field of complex numbers.

Theorem. *The necessary and sufficient conditions for a non-empty sub-set F' of a field F to be a sub-field of F are*

(*i*) $a \in F', b \in F' \Rightarrow a - b \in F'$,

(*ii*) $a \in F', 0 \neq b \in F' \Rightarrow ab^{-1} \in F'$.

Let F' be a sub-field of the field F. Now F' is a group with respect to addition. Therefore $b \in F' \Rightarrow -b \in F'$.

Also F' is closed with respect to addition.

Therefore $a \in F', b \in F' \Rightarrow a+(-b) \in F' \Rightarrow a-b \in F'$.

Now each non-zero element of F' possesses a multiplicative inverse.

Therefore $0 \neq b \in F' \Rightarrow b^{-1} \in F'$.

But F' is closed with respect to multiplication.

Therefore $a \in F', 0 \neq b \in F' \Rightarrow ab^{-1} \in F'$.

Hence the conditions are *necessary*.

To prove that the conditions are also *sufficient*, we assume that F' is a non-empty sub-set of F and the above two conditions are satisfied.

As in the case of sub-rings, we can show, by the first given condition, that $(F',+)$ is an abelian group.

Now, let $a(\neq 0) \in F'$. Then, from the second condition, we have

$$0 \in F', 0 \neq a \in F' \Rightarrow aa^{-1} \in F' \Rightarrow 1 \in F'.$$

Now $1 \in F'$; therefore, again by the second given condition, we have $1 \in F', 0 \neq a \in F' \Rightarrow 1a^{-1} \in F' \Rightarrow a^{-1} \in F'$.

Therefore each non-zero element of F' possesses a multiplicative inverse.

Now, let $a \in F'$ and $0 \neq b \in F'$; then $b^{-1} \in F'$.

From the second condition, we have

$$a \in F', 0 \neq b^{-1} \in F' \Rightarrow a\left(b^{-1}\right)^{-1} \in F' \Rightarrow ab \in F'.$$

Also, if $b = 0$, then $ab = 0$ and $0 \in F'$.

Therefore $ab \in F'$, for all $a, b \in F'$.

The associative law of multiplication and distributive law of multiplication over addition hold in F and hence these will hold in F' also.

Hence F' is a sub-field of F.

4.15. Ideals.

A non-empty sub-set S of a ring $(R, +, \cdot)$ is called a *left ideal* of R, if (i) $(S,+)$ be a sub-group of R and (ii) $rs \in S \forall\ r \in R$ and $\forall\ s \in S$.

A non-empty sub-set S of a ring $(R, +, \cdot)$ is called *a right ideal* of R, if (i) $(S,+)$ be a sub-group of R and (ii) $sr \in S \forall\ r \in R$ and $\forall\ s \in S$.

A non-empty sub-set S of a ring $(R, +, \cdot)$ is said to be an *ideal* (also a two- sided ideal), if and only if it is both a left ideal and a right ideal.

Thus a non-empty sub-set S of a ring $(R, +, \cdot)$ is said to be an ideal of R, if (*i*) S be a sub-group of R under addition

and (*ii*) $rs \in S$ and $sr \in S$ for every $r \in R$ and for every $s \in S$.

From the definition, it is clear that the ideal S is necessarily a sub-ring of the ring R.

For, $(S, +)$ is a group and $a, b \in S \Rightarrow a - b \in S$.

Also $rs \in S$, $sr \in S \ \forall \ r \in R$ and $\forall \ s \in S$

imply $rs \in S$ and $sr \in S \ \forall \ r \in S$ and $\forall \ s \in S$ as $S \subseteq R$.

But every sub-ring S of a ring R is not an ideal ; for, if S be a sub-ring of R, we have $rs \in S \ \forall \ r, s \in S$ which does not imply

$$rs \in S \forall \ r \in R \text{ and } \forall \ s \in S.$$

Every ring possesses two improper ideals, one is the ring R itself and the other is the singleton $\{0\}$. The former is known as the *unit ideal* and the latter the *zero ideal* or the *null ideal*. Any other ideal is known as proper ideal. A ring is called a *simple ring*, if it has no proper ideals.

For a commutative ring $(R, +, \cdot)$, the left ideal, the right ideal and the two sided ideal coincide.

The sub-set nZ of all integral multiples of a fixed $n \in Z$ is an ideal of the ring Z. nZ is a sub-ring of Z. It is an ideal of Z, since, by multiplying an element of nZ by any integer, we get an element of nZ.

Z is the sub-ring of $(Q, +, \cdot)$, but it is not an ideal, since $1 \in Z$ and $\frac{3}{2} \in Q$ but $1 . \frac{3}{2} = \frac{3}{2} \notin Z$.

Similarly, the sub-ring Q of R is not an ideal of R.

For a commutative ring R, an ideal P of $R, (P \neq R)$, is said to be a *prime ideal* of R, if $ab \in P$ when $a, b \in R$ implies that either $a \in P$ or $b \in P$. The null ideal $\{0\}$ in the ring formed by the set Z of integers is a prime ideal, since $ab \in \{0\}$ when $a, b \in Z$ implies $ab = 0$, which implies either $a = 0$ or $b = 0$, which implies that either $a \in \{0\}$ or $b \in \{0\}$.

In a commutative ring R, an ideal M of $R, (M \neq R)$, is said to be a *maximal ideal* of R, if whenever U is an ideal of R such that $M \subset U \subset R$, then either $U = M$ or $U = R$. The zero ideal is a maximal ideal in a simple ring. The zero ideal of a ring R is maximal if and only if R be a field.

Theorem 1. *The intersection of two ideals is an ideal.*

Let S and T be two ideals of the ring $(R, +, \cdot)$. Hence $(S, +)$ and $(T, +)$ are sub-groups of R. Therefore $S \cap T$ is also a sub-group of R under addition.

Now $s \in S \cap T \Rightarrow s \in S$ and $s \in T$.

Also S is an ideal. Hence

$$sr \in S \text{ and } rs \in S \ \forall r \in R \text{ and } \forall s \in S.$$

Again T is an ideal. Hence

$$rs \in T \text{ and } sr \in T \ \forall r \in R \text{ and } \forall s \in T.$$

Now $sr \in S, sr \in T \Rightarrow sr \in S \cap T$

and $rs \in S, rs \in T \Rightarrow rs \in S \cap T$.

Therefore $sr \in S \cap T$ and $rs \in S \cap T \ \forall r \in R$ and $\forall s \in S \cap T$.

Hence $S \cap T$ is an ideal of R.

Cor. The intersection of all ideals of a ring R containing a non-empty sub-set S is an ideal of R and it is the smallest ideal of R containing S and is said to be the ideal generated by S. When S is a single element of R, then the ideal generated by S is said to be a *principal ideal* of R. Thus the smallest ideal of R containing the element a $(a \in R)$ is a principal ideal of R. The null ideal $\{0\}$, being the smallest ideal of R containing the element 0, is a principal ideal of R. Every ideal of the ring, formed by the set of integers, is a principal ideal of the ring.

A ring, in which every ideal is principal, is called a *principal ideal ring*. Thus the ring formed by the set of integers is a principal ideal ring.

Theorem 2. *A field has no proper ideals.*

Here we are to show that either $S = \{0\}$ or $S = F$, where S is an ideal of a field F.

Let S be non-zero in F. If a be any non-zero element of S, then $1 = a^{-1}a \in S$, since S is an ideal.

Again $1 \in S, x \in F \Rightarrow x.1 = x \in S$.

This shows that each element of the field F belongs to S, so that $F \subseteq S$.

But $S \subseteq F$. Hence $S = F$.

4.16. Factor rings.

Let I be an ideal of the ring R and R/I denote the set of cosets of I in R.

If $(x+I)$ and $(y+I)$ be cosets of I in R and two binary operations be defined on R/I as follows:

$(x+I)+(y+I)=(x+y)+I$ and $(x+I)(y+I)=xy+I$, for all x, y in R, then the binary operations are well-defined and under these operations, R/I is a ring. This ring is said to be a *factor ring* of R. Some authors call it a *quotient ring* of R. For example, $nZ = \{nx | x \in Z\}$, for each $n \in Z$, is an ideal of Z and Z/nZ is a factor ring of Z.

4.17. Field of quotients.

Any integral domain D can be embedded in (or enlarged to) a field F such that every element of F can be expressed as a quotient of two elements of D. Such a field F is said to be a *field of quotients* of D. For example, the integers are contained in the field Q of rational numbers, whose elements can all be expressed as quotients of integers.

4.18. Homomorphism and isomorphism of rings.

Let R and S be two rings. A mapping $f : R \to S$ is said to be a *homomorphism* from R to S, if

$f(a+b)=f(a)+f(b)$ and $f(a.b)=f(a).f(b)$, for all $a, b \in R$.

Here the operations '+' and '$\bullet$', occurring on the left hand side, are on R where as those on the right hand side are on S. If R/I be a factor ring of R, I being an ideal of the ring R, then the mapping $R \to R/I$ given by $x \to x+I$ $(x \in R)$ is a homomorphism of R onto R/I with kernel I.

A sub-set of R given by $\{a \in R : f(a) = 0'\}$, where $0'$ is the zero element of S, is called the *kernel* of f and is written as $\ker f$. Thus $\ker f$ is the set of elements of R that map to zero. Also $\ker f$ is an ideal of R.

Some properties of homomorphisms

Let f be a homomorphism of a ring R to a ring S.

(i) If 0 be the additive identity in R, then $f(0) = 0'$ is the additive identity of S.

(ii) $f(-a) = -f(a)$, for all $a \in R$.

Let $a \in R$.

Then $a + (-a) = (-a) + a = 0$ in R.

We have $f(0) = f\{a + (-a)\} = f(a) + f(-a)$

and also $f(0) = f\{(-a) + a\} = f(-a) + f(a)$.

Therefore $f(a) + f(-a) = f(-a) + f(a) = 0'$, which implies $f(-a)$ is the additive inverse of $f(a)$ in S.

Hence $f(-a) = -f(a)$.

(iii) If A be a sub-ring of R, then $f(A)$ is a sub-ring of S and if B be a sub-ring of S, then $f^{-1}(B)$ is a sub-ring of R.

(iv) If R be commutative, then $f(R)$ is commutative.

(v) If R has a unity 1, $S \neq \{0\}$ and f is onto, then $f(1)$ is the unity of S.

All these properties can be established using the corresponding group properties.

Let the mapping f be a homomorphism from R to S. If the mapping f be injective, then the homomorphism is said to be a *monomorphism*. When the mapping f is surjective, then the homomorphism is said to be an *epimorphism*. If the mapping f be bijective, then the homomorphism is said to be an *isomorphism*.

4.19. Isomorphism theorems for rings.

First theorem. *If R and S be two rings and $f : R \to S$ be an epimorphism with kernel K, then the ring S is isomorphic to the factor ring R/K.*

In other words, if f be a homomorphism of a ring R onto a ring S with kernel K, then R/K and S are isomorphic.

It is also known as *fundamental theorem of ring homomorphism.*

Second theorem. *If S be a sub-ring of a ring R and I be an ideal of R, then the factor rings $(S + I)/I$ and $S/(I \cap S)$ are isomorphic.*

Here we define $g : S \to (S+I)/I$ by $g(x) = x + I$, $x \in S$, so that g is an epimorphism. If K be the kernel of g, then, by the first isomorphism theorem, S/K is isomorphic to $(S+I)/I$. Since ker g is an ideal of S, so $K = I \cap S$ and hence the theorem follows.

Third theorem. *If I and J be two ideals of a ring R with $J \subseteq I$, then I/J is an ideal of R/J and $(R/J)/(I/J)$ is isomorphic to R/I.*

4.20. Illustrative Examples.

Ex.1. *If D be an integral domain, then show that the non-zero elements of D form a commutative semi-group under multiplication.*

Assume that $\bar{D} = D - \{0\}$. ... (1)

Let $a, b \in \bar{D}$; then $a, b \in D$.

Now, D being closed under multiplication, we have $ab \in D$.

We have again $ab \neq 0$, as a and b are non-zero elements and D contains no divisor of zero; hence we have $ab \in \bar{D}$. This shows that $\bar{D}$ is closed under multiplication.

Now, since multiplication is associative and commutative on D, it is associative and commutative on $\bar{D}$, as $\bar{D}$ is a sub-set of D, from (1).

Hence $(\bar{D}, \cdot)$ is a commutative semi-group.

Ex. 2. *(a) If D be an integral domain and a be an element of D such that $a^2 = a$, then prove that $a = 0$ or $a = 1$.*

(b) If the characteristic of an integral domain D be a non-zero number p, then prove that the order of every non-zero element in the group $(D, +)$ is p.

(a) Here a is an element of D such that $a^2 = a$; then $a(a-1) = 0$ and hence $a = 0$ or $a = 1$, as D is an integral domain.

[An element x of a ring is *idempotent*, if $x^2 = x$.]

(b) p being the characteristic of an integral domain, $p(\neq 0)$ is a prime number.

Let a be a non-zero element of D.

Then $pa = a + a + \cdots\cdots + (p \text{ terms})$

$= (1 + 1 + \cdots\cdots + 1) \cdot a$, 1 being the unity

$= (p1) \cdot a = 0 \cdot a = 0$.

This shows that the order of a in the group $(D, +)$ is a divisor of p. Now, p being a prime number, its only divisors are p and 1. The zero element in the group is the only element of order 1. Hence the order of a is p.

Ex. 3. *Prove that the set of all real numbers of the form* $(a+b\sqrt{2})$, *where a and b are rational numbers, is a field under usual addition and multiplication.*

[B.H. 1994]

Let $S=\{(a+b\sqrt{2}),(c+d\sqrt{2}),(e+f\sqrt{2}),.....\}$,

where $a, b, c,.....$ are all rational numbers.

We observe that

(*i*) $(a+c)+(b+d)\sqrt{2}\in S$ (closed for addition)

as $(a+c)$ and $(b+d)$ are rational numbers ;

(*ii*) $\left[(a+b\sqrt{2})+(c+d\sqrt{2})\right]+(e+f\sqrt{2})$

$=(a+c+e)+(b+d+f)\sqrt{2}$

$=(a+b\sqrt{2})+\left[(c+d\sqrt{2})+(e+f\sqrt{2})\right]$ (associative) ;

(*iii*) $(a+b\sqrt{2})+(0+0\sqrt{2})=(0+0\sqrt{2})+(a+b\sqrt{2})=a+b\sqrt{2}$,

so that $(0+0\sqrt{2})$ is the additive identity which belongs to S ;

(*iv*) $(a+b\sqrt{2})+(-a-b\sqrt{2})=(-a-b\sqrt{2})+(a+b\sqrt{2})=0+0\sqrt{2}$,

so that additive inverse exists for each element of S ;

(*v*) $(a+b\sqrt{2})+(c+d\sqrt{2})=(c+d\sqrt{2})+(a+b\sqrt{2})$,

so that commutative law holds ;

(*vi*) $(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+\sqrt{2}(ad+bc)\in S$,

as $(ac+2bd)$ and $(ad+bc)$ are rational numbers.

We can easily verify that the associative law for multiplication holds and multiplication distributes addition.

Also we can verify that the commutative law holds good for multiplication.

Thus S forms a commutative ring.

Clearly, the commutative ring is seen to possess the unity element, the multiplicative identity being $(1+0\sqrt{2})\in S$.

Again we have, if $a+b\sqrt{2} \neq 0+0\sqrt{2}$, then

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2} \in S,$$

since $\frac{a}{a^2-2b^2}$ and $-\frac{b}{a^2-2b^2}$ are rational numbers, as a and b are rational.

Also $\left(\frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2}\right).\left(a+b\sqrt{2}\right)$

$$= \left(a+b\sqrt{2}\right).\left(\frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2}\right) = 1 .$$

Thus the multiplicative inverse of $\left(a+b\sqrt{2}\right)$ is

$\left(\frac{a}{a^2-2b^2} - \sqrt{2}\frac{b}{a^2-2b^2}\right)$, which belongs to S.

Hence S forms a commutative ring with unity element and every non-zero element belonging to S has a multiplicative inverse belonging to S.

Hence the set S forms a field.

[This field is usually denoted by $Q\left(\sqrt{2}\right)$.]

Ex. 4. *Prove that the set of all 2×2 real matrices of the form $\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$ forms a field with respect to matrix addition and multiplication.* [B.H. 1982; C.H.1992]

Let the set be S and A, B be two elements of S given by

$$A = \begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix}, \quad B = \begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}.$$

Now $A+B = \begin{bmatrix} x_1+x_2 & y_1+y_2 \\ -(y_1+y_2) & x_1+x_2 \end{bmatrix}$, showing that $A+B \in S$.

Hence S is closed under matrix addition.

The associative property holds for addition, as it holds for all 2×2 matrices.

We have the matrix $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ in S, which is the additive identity.

For the additive inverse of A, we see that

$$-A=\begin{bmatrix} -x_1 & -y_1 \\ -(-y_1) & -x_1 \end{bmatrix}$$

is in S, and is the additive inverse of A in S.

Furthermore $\{S, +\}$ is an abelian group, as the commutative property holds good in S for all 2×2 real matrices.

Thus S forms a field under matrix addition.

For matrix multiplication, we see that

$$A.B=\begin{bmatrix} x_1 & y_1 \\ -y_1 & x_1 \end{bmatrix}\cdot\begin{bmatrix} x_2 & y_2 \\ -y_2 & x_2 \end{bmatrix}=\begin{bmatrix} x_1x_2-y_1y_2 & x_1y_2+x_2y_1 \\ -(x_1y_2+x_2y_1) & (x_1x_2-y_1y_2) \end{bmatrix}.$$

Therefore $A.B\in S$. Hence S is closed under matrix multiplication. The associative property of multiplication holds in S, as it holds for all 2×2 matrices.

The multiplicative identity for S is $I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $I\in S$.

We observe that A is non-singular, since $\det A=x_1^2+y_1^2\neq 0$, as x_1 and y_1 are not both zero.

Hence A^{-1} exists and $A^{-1}=\dfrac{1}{x_1^2+y_1^2}\begin{bmatrix} x_1 & -y_1 \\ y_1 & x_1 \end{bmatrix}$.

Thus $A^{-1}\in S$, which is the multiplicative inverse of A, since

$$A.A^{-1}=A^{-1}.A=I.$$

We have $A.B=B.A$ and hence multiplication is commutative. As the distributive property holds for 2×2 real matrices, the property holds in S. Hence S forms a field under matrix multiplication.

Ex. 5. *For the set* $\{0, 1, 2, 3, 4\}$, *show that the modulo* 5 *system is a field.*

We construct the addition modulo 5 and multiplication modulo 5 tables.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

From the tables we observe the following :

(*i*) The system is closed under the operation of addition modulo 5 and multiplication modulo 5.

(*ii*) Addition and multiplication are commutative in the modulo 5 system.

(*iii*) 0 is the identity element for addition modulo 5 and 1 is the identity element for multiplication modulo 5.

(*iv*) Each element in the modulo 5 system has an additive inverse. Every element, except 0, has a multiplicative inverse.

(*v*) Addition modulo 5 and multiplication modulo 5 are associative.

(*vi*) Multiplication modulo 5 distributes over addition modulo 5.

Thus the modulo 5 system is a field.

Ex. 6. *If a, b be two elements of a field F and $b \neq 0$, then prove that $a = 1$, if*

$$(ab)^2 = ab^2 + bab - b^2. \qquad \text{[C.H. 1991 ; V.H. 1998]}$$

We have $(ab)(ab) = (ab)b + bab - bb \Rightarrow aba = ab + ba - b$, since $b \neq 0$

$$\Rightarrow aab = 2ab - b$$

$$\Rightarrow aab = (2a-1)b$$

$$\Rightarrow aa = 2a - 1, \text{ since } b \neq 0.$$

This gives $aa - a - a + 1 = 0 \Rightarrow (a-1)(a-1) = 0$

$$\Rightarrow a - 1 = 0.$$

Hence $a = 1$.

Ex. 7. *If $R = (Z, +, \cdot)$ be a ring and the mapping $f : R \to R$ be defined by $f(x) = -x$, $x \in Z$, then show that f is not a homomorphism.*

Let $a, b \in Z$. Then $a \cdot b \in Z$ and $f(a \cdot b) = -ab$.

But $f(a) \cdot f(b) = (-a) \cdot (-b) = ab \neq f(a \cdot b)$.

Hence f is not a homomorphism.

Ex. 8. *Let R be a ring with unity 1 and $f : R \to S$ be a ring homomorphism. If $f(1) = 0$, then show that ker $f = R$.*

Let $a \in R$. Then $f(a) = f(a \cdot 1) = f(a) \cdot f(1) = 0$.

Therefore $f(a) = 0$ for all $a \in R$, which shows that

$$\ker f = R.$$

Examples IV (B)

1. (*a*) Show that the zero element is 0 and the unit element is 1 for the integral domains given by $(Q, +, \cdot)$ and $(R, +, \cdot)$.

(*b*) Show that the ring of integers is an integral domain.

(*c*) Show that the set of numbers of the form $\left(a + b\sqrt{2}\right)$, where a, b are integers, does not form an integral domain under ordinary addition and multiplication.

2. (*a*) Prove that the set of all even integers forms a commutative ring but not a field.

(*b*) Show that the set of all rational numbers is a field with respect to addition and multiplication.

3. Prove that a finite commutative ring without zero divisor is a field. [*C.H. 1986, 1994*]

4. (*a*) Show that a set of all integers forms an integral domain but not a field. [*K.H. 1990*]

(*b*) Prove that there is no integral domain of order 6.

5. Show that, in a field F,

(*i*) $(-a)b = -(ab)$, $a, b \in F$; (*ii*) $(-a)(-b)^{-1} = ab^{-1}$, $a, b \in F$;

(*iii*) $\left(a^{-1}\right)^{-1} = a$; (*iv*) $(-a)^{-1} = -\left(a^{-1}\right)$. [*C.H. 2005*]

6. Verify that a set of complex numbers forms a field with respect to usual addition and multiplication.

7. Prove that the equations $a.\, x = b$ and $y.a = b$ have unique solutions in a field, where $a, b \in F$ and $a \neq 0$.

8. (*a*) If $a, b \in F$ and $a \neq 0$, then show that there exists a unique element x, such that $a.x = b$.

[Since $a.\left(a^{-1}b\right) = \left(a.a^{-1}\right)b = eb = b$, therefore $x = a^{-1}b$.

Prove the uniqueness.]

(*b*) If $a, b, c \in F$ and $a \neq 0$, then show that the equation $ax + b = c$ has a unique solution in F. [*C.H. 2008*]

9. Show that the set of numbers of the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, where $a, b, c \in Q$, is a field under usual addition and multiplication.

10. (*a*) In a field F, prove that

$a^2 = b^2 \Rightarrow$ either $a = b$ or $a = -b$, $a, b, \in F$. [*C.H. 1986,1996*]

(*b*) If $a,b,c,d \in F$, then show that $\frac{a}{b}=\frac{c}{d} \Rightarrow ad = bc$. [N.B.H. 2001]

$\left[\frac{a}{b}=\frac{c}{d} \Rightarrow ab^{-1}=cd^{-1} \Rightarrow b^{-1}a=cd^{-1} \Rightarrow bb^{-1}a=bcd^{-1} \Rightarrow a=bcd^{-1}.\right]$

11. Let $T = Q \times Q = \{(a,b) : a,b \in Q$, the field of rational numbers.$\}$

In T, define addition '+' and multiplication '$\bullet$' by

$(a,b)+(c,d)=(a+c,b+d)$ and $(a,b)\bullet(c,d)=(ac, bd)$.

Show that T is a commutative ring but not a field. [C.H. 1987]

12. Show that the set $S = \{0,1,2,3\}$ forms a ring under the addition and multiplication modulo 4, but is not a field.

13. Show that the set $S = \{0,1\}$ under the addition and multiplication modulo 2 is a field. Show further that the set $S = \{0,1,2\}$ forms a field under the addition and multiplication modulo 3.

14. Show that the modulo seven system is a field but the modulo six system is not a field.

15. Show that the set $S = \{0,1,2,3,4,5,6,7\}$ is a ring under the addition and multiplication modulo 8. Show also that the ring is commutative but is not an integral domain.

[$2, 4 \in S$ are two non-zero elements such that $2.4 \equiv 0$.]

16. Let S be a set of all square matrices of the form $\begin{bmatrix} 0 & 0 \\ a & b \end{bmatrix}$, where a and b are integers. Show that S is a ring and not a field.

17. Show that the set of all 2×2 matrices $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, where $a,b \in R$, is not a field with respect to matrix addition and multiplication. [C.H.1994.2005]

18. Show that the ring of matrices $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$ does not form a field, if $a,b \in R$, but it does, if $a,b \in Q$.

19. Show that the set of matrices of the form $\begin{bmatrix} a & b \\ 2b & a \end{bmatrix}$, with rational a,b, forms a field under usual addition and multiplication of matrices. [C.H.1981]

20. (*a*) Show that the set S of real matrices of the form $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ is a right ideal of the ring R of all the square matrices of order 2.

(*b*) Prove that the set of real matrices of the form $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ is a left ideal of the ring of all square matrices of order 2.

(*c*) R is the set of all 2×2 matrices over Z. Prove that

$$S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}; a, b \in Z \right\}$$

is neither a right ideal nor a left ideal in R.

21. If S be an ideal of R and $I \in S$, then prove that $S = R$.

22. R is a commutative ring. Show that the set of all nilpotent elements in R is an ideal in R.

23. R is a finite commutative ring with unity. Show that every prime ideal in R is a maximal ideal in R.

24. (*a*) Show that the set of numbers of the form $\left(a + b\sqrt{2}\right)$, $a, b \in Q$ is a sub-field of the field of real numbers. [*T.H. 2003*]

(*b*) In the field R of all real numbers, show that the set $A = \{a + b\sqrt{3} \in R : a, b$ are rational numbers $\}$ is a sub-field but the set $B = \{b\sqrt{3} \in R : b$ is a rational number $\}$ is not a sub-field. [*C.H. 1997*]

[Let $a_1 + b_1\sqrt{3}, a_2 + b_2\sqrt{3} \in A$. Then $\left(a_1 + b_1\sqrt{3}\right) - \left(a_2 + b_2\sqrt{3}\right) \in A$ and $\frac{a_1 + b_1\sqrt{3}}{a_2 + b_2\sqrt{3}} \in A$. Let $b_1\sqrt{3}, b_2\sqrt{3} \in B$. Then $\frac{b_1\sqrt{3}}{b_2\sqrt{3}} = \frac{b_1}{b_2} \notin B$.]

(*c*) Prove that the set $A = \left\{a + b\omega : a, b \in R\right\}$ is a sub-field of the field of complex numbers. [*B.H. 2004 ; N.B.H.2011*]

25. (*a*) Show that a commutative ring D is an integral domain, iff, for $a, b, c \in D$ with $a \neq 0$, $ab = ac \Rightarrow b = c$.

(*b*) Show that the ring I of integers (mod p) is an integral domain, if and only if p be prime.

26. Prove that the set of all 2×2 matrices of the form

$$\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix},$$

where a, b, c, d are arbitrary real numbers, forms a division ring and not a field.

27. Show that the set of classes of residue (mod g) is a ring and this ring is a field, if g be prime.

28.(a) S and T are two ideals of a ring R. Prove that the sub-set $(S + T)$ defined by $S+T=\{a+b : a \in S, b \in T\}$ is an ideal of R.

(b) Prove that the set of matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $a,b \in Z$ is a sub-ring of $M_2(Z)$ but not an ideal of $M_2(Z)$.

29. R is a ring with unity 1. If P be an ideal of R containing a unit element a of R, then show that $P = R$.

30. (a) Prove that an ideal of a ring R is a sub-group of the additive group R^+.

(b) If F be a field, then show that the field of quotients of F is a ring isomorphic to F.

31. (a) If R be a ring with unit element 1 and ϕ be a homomorphism of R onto R', then prove that ϕ (1) is the unit element of R'.

(b) Show that a homomorphism from a field onto a ring with more than one element must be an isomorphism.

(c) If R, S, T be three rings and $f : R \to S$ and $g : S \to T$ be given homomorphisms, then prove that $g \circ f$ is a homomorphism from R to T.

32. If $R=\left\{\begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in Z\right\}$ and $f : R \to Z$ be defined by

$f\begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b$, then show that f is a ring homomorphism and $R/\ker f$ is isomorphic to Z. Show that $\ker f$ is a prime ideal of R but not a maximal ideal in R.